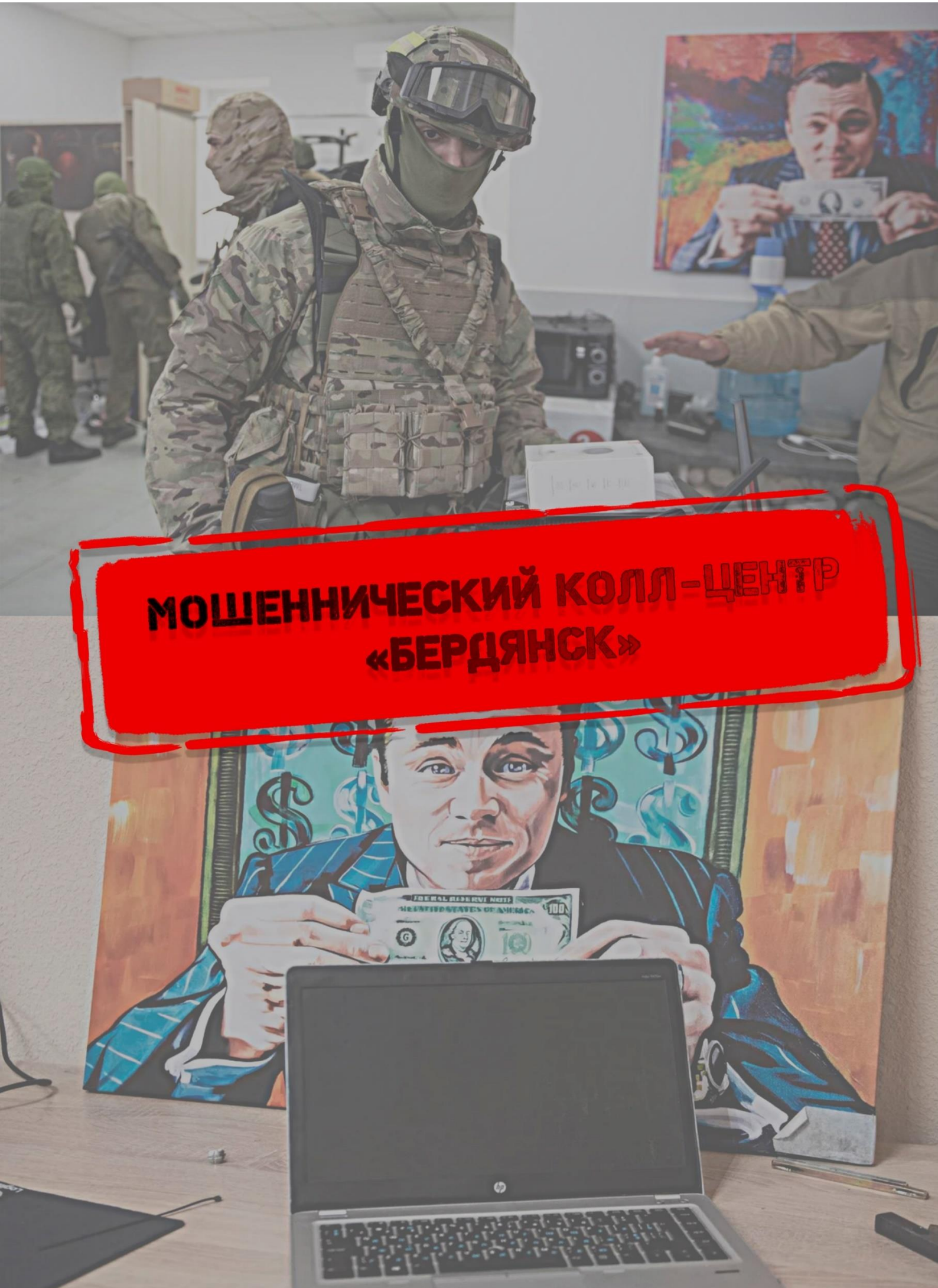


МОШЕННИЧЕСКИЙ КОЛЛ-ЦЕНТР «БЕРДЯНСК»

СОДЕРЖАНИЕ

«Война есть просто продолжение политики другими средствами».

К. Клаузевиц

ВВЕДЕНИЕ

Сегодня в России сложно найти человека, которому хотя бы раз не звонили из мошеннического call-центра с целью хищения денежных средств с банковских карт и счетов. Из многочисленных публикаций в СМИ[1, 2, 3], признаний самих преступников[4, 5] и комментариев правоохранительных органов[6, 7] следует, что большинство таких call-центров расположены на Украине, где они действуют не первый год. Еще в 2019 году заметная часть мошеннических звонков на российские номера поступала именно оттуда[8]. За это время граждане России, по разным оценкам экспертов, перевели мошенникам, работающим на украинские call-центры, десятки миллиардов рублей[9].

По данным Сбера, основные call-центры располагаются в г.Днепр, который неофициально считается столицей телефонного мошенничества[10]. На Украине создана максимально комфортная среда для работы преступников: значительная криминализация общества, тотальная коррупция, покровительство преступлениям против граждан России со стороны государственных структур.

В какой-то момент количество call-центров в г. Днепр достигло отметки в 1100, а телефонным обзвоном было занято значимая часть населения в возрасте до 35 лет. Со временем call-центры, работающие по классическим схемам обмана «звонок из службы безопасности банка», закрылись, их

---

[1] https://iz.ru/925899/anna-kaledina/movy-ton-telefonnye-moshenniki-perebiraiutsia-na-ukrainu

[2] https://www.rbc.ru/society/19/11/2021/6196f8799a7947f73fa87b72

[3] https://news.ru/economics/nazvan-ukrainskij-gorod-otkuda-postupaet-tret-moshennicheskih-zvonkov/

[4] https://msk1.ru/text/criminal/2022/08/30/71590385/

[5] https://vz.ru/news/2021/4/8/1093496.html

[6] https://www.rbc.ru/rbcfreenews/62fe3cae9a7947bf822dbc9b

[7] https://ria.ru/20211015/moshenniki-1754548265.html

[8] см. сноску 1

[9] https://www.spb.kp.ru/daily/27377/4571027/

[10] https://www.banki.ru/news/lenta/?id=10954136

количество сократилось до 150 – остались только наиболее профессиональные. При этом call-центры получили широкое распространение во всех крупных городах Украины – в Харькове, Запорожье, Одессе, Бердянске и пр.

По оценке Сбера, на сегодняшний день общее количество мошеннических call-центров по всей Украине превышает 3000 шт. Схемы обмана стали многоэтапными и растянутыми во времени, когда диалог с клиентом может продолжаться в течение нескольких дней. Зачастую злоумышленники возвращаются к обманутым гражданам, чтобы обмануть их повторно.

Речь идет о целой криминальной индустрии, в которую вовлечены тысячи людей помимо непосредственно сотрудников call-центров. Эти люди активно вовлечены в пособничество организаторам противоправной деятельности. Так, например, риелторы подыскивают площади под call-центры (арендная плата за мошеннический офис в среднем на 30-40% выше, чем за помещение для любого другого вида деятельности). Компьютерные фирмы занимаются продажей и настройкой оборудования «под ключ». Координаторы, отвечающие за выдачу зарплаты сотрудникам call-центров, регулярно посещают пункты обмена валют, в том числе и криптообменники. Службы доставки еды (в рабочий день около 50% сотрудников сервисов доставки «Глово» и «Ракета») выполняют заказы тысяч сотрудников call-центров.

Долгое время детали работы мошеннических call-центров были скрыты от экспертного сообщества, однако, в рамках Специальной военной операции (СВО) эксперты получили для анализа информацию, хранившуюся на компьютерах одного из call-центров в г.Бердянск.

Имеющийся у Сбера опыт в противодействии мошенничеству помог в расследовании: анализе данных, сборе доказательственной базы, обобщении информации из открытых источников, комментариев экспертов и прочих данных, полученных исследователями из компьютеров call-центра в г.Бердянск. В данном отчете дана оценка масштабов деятельности украинских call-центров по обману граждан РФ, раскрыты детали организации работы типового call-центра (организационная структура, процессы поиска и найма сотрудников, получения данных о гражданах РФ, сценарии разговора, применяемые технологии и пр.).

Установленные данные сотрудников бердянского call-центра, их роли и используемые инструменты позволили правоохранительным органам установить личности всех злоумышленников и объявить их в розыск. Собранная в ходе исследования информация передана в правоохранительные органы для проведения необходимых мероприятий по привлечению

преступников к ответственности. В данный момент заведено более тысячи уголовных дел.

Уверены, что информация, содержащаяся в данном отчете, поможет правоохранительным органам в разработке эффективных предложений по защите граждан РФ от телефонного мошенничества, в более качественном расследовании преступлений, а также позволит повысить бдительность и уровень киберграмотности граждан.

1. ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО В РОССИИ

1.1. Оценка ущерба от противозаконной деятельности call-центров

За последние несколько лет на территории России наблюдается рост числа дистанционных преступлений – телефонного мошенничества, которое реализуется методами социальной инженерии. Так, по данным Банка России[11], во II квартале 2022 года граждане РФ под воздействием третьих лиц перевели злоумышленникам денежные средства 211 тыс. раз, что в сумме составило 2,8 млрд. руб.

Также со второго квартала 2021 г. до второго квартала 2022 г. количество мошеннических номеров с использованием 8-800 выросло с 208 до 277 единиц (на 33%), городских – с 8,4 тыс. до 41,4 тыс. (на 389%), мобильных – с 3,1 тыс. до 75,8 тыс. (на 2296%)[12].

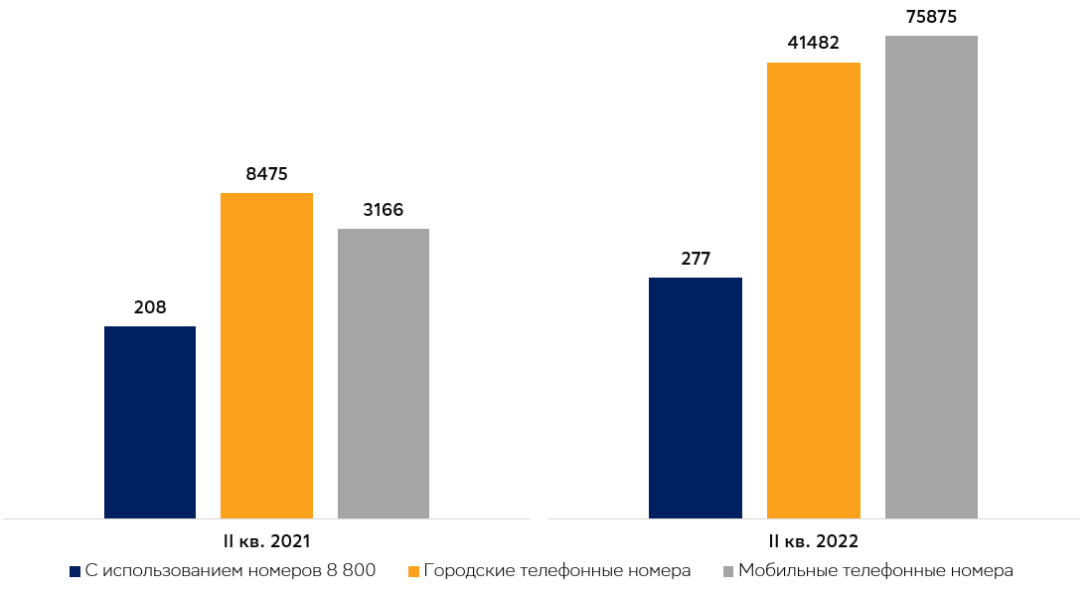


Рисунок 1. Выявленные мошеннические телефонные номера

[11] Отчет Банка России за 2 квартал 2022 - http://www.cbr.ru/analytics/ib/review_2q_2022/

[12] См. сноску 11.

При этом, реальная картина финансовых потерь превышают статистику Банка России в разы – в соответствии со статистикой МВД России и данными от экспертов в области кибербезопасности, объем мошенничества в РФ сегодня оценивается от 55 (оценка МВД) до 150 млрд. рублей (оценка экспертов) в год. По данным Сбера, на социальную инженерию приходится 90% всех финансовых преступлений, из которых 94% — это телефонное мошенничество[13].

Начало растущего тренда по телефонному мошенничеству фиксируется в России с 2017 года. Уже через год представители финансово-кредитной системы стали отмечать значительное увеличение количества совершаемых хищений у клиентов банков. Это обусловлено применением злоумышленниками простой и доступной технологии подмены номера, когда в качестве номера звонящего подставляется официальный телефон банка. Фактически России была объявлена негласная «телефонная война». Пик проблемы пришелся на 2020 год – только по данным Сбера с жалобами на попытки мошенничества в банк обратилось более 3,7 млн. клиентов[14]. При этом, в одном из кейсов максимальная сумма, похищенная у одного из коммерческих банков РФ, составила 5.4 млн. долларов США и обналичивалась в несколько этапов.

По нашей оценке, тренд на дальнейший рост телефонного мошенничества сохранял актуальность вплоть до начала специальной военной операции. В январе 2022 года клиенты Сбера 250 тысяч раз пожаловались в банк на мошенничество, в феврале было зафиксировано 264 тысячи обращений – на 6% больше. После 24 февраля 2022 года зафиксирована полная остановка «мошеннического конвейера». Однако, через месяц начался плавный рост звонков, но их объемы были уже существенно ниже: если до спецоперации количество жалоб составляло в среднем 11 тыс. в сутки, то с 20 марта 2022 года – 2 тыс. в сутки, снижение в 5,5 раз[15].

По оценкам МВД и банков, количество звонков составляет до 100 тыс. в сутки[16]. В 99% случаев злоумышленники используют IP-телефонию и подмену абонентского номера на российскую нумерацию – 495/499 и def-нумерацию сотовой связи. По итогам 2022 года экспертами прогнозируется, что количество жалоб на мошеннические звонки составит более 4.5 млн. шт., а официальный объем мошенничества в РФ (объем, который сами банки

[13] https://ria.ru/20220416/kiberataki-1783857919.html

[14] https://ria.ru/20210601/sberbank-1735112983.html

[15] https://ria.ru/20220418/kuznetsov-1784035779.html

[16] https://www.mk.ru/social/2021/04/15/telefonnoe-moshennichestvo-v-cifrakh-skolko-aferisty-zarabatyvayut-na-obmane-rossiyan.html

заявляют в Банк России в рамках обязательной отчетности) может превысить 15 млрд. рублей. Не официальный – порядка 165 млрд.

По экспертной оценке Сбера, сегодня на долю Украины приходится до 90% всех call-центров, работающих против граждан РФ, остальные располагаются на территории России и стран СНГ. Общий объем похищенных средств украинскими call-центрами достигал 75 млрд. руб. в 2020 году, из которых 65% выводились непосредственно call-центрами, принадлежащими днепропетровским организованным преступным группам (ОПГ).

1.2. Предпосылки возникновения мошеннических call-центров на территории Украины

На территории Украины действует сеть мошеннических call-центров, о чем неоднократно публиковались расследования в средствах массовой информации, таких как международная сеть расследований OCCRP [17], шведская газета Dagens Nyheter [18], европейские СМИ [19], специальные репортажи российской телепередачи «Андрей Малахов. Прямой эфир» [20], украинские информационные агентства[21] и многие другие.

Рисунок 2. Скриншот статьи шведской газеты Dagens Nyheter от 01.03.2020

[17] https://www.occrp.org/en/fraud-factory/trail-of-broken-lives-leads-to-kyiv-call-center

[18] https://www.dn.se/nyheter/sverige/fraudfactory//

[19] https://emerging-europe.com/news/ukraine-is-failing-to-tackle-its-scam-call-centres/

[20] https://smotrim.ru/video/2312392, https://smotrim.ru/video/2355806, https://smotrim.ru/video/2362918.

[21] https://com1.org.ua/moshennycheskye-call-tsentry/

Аналогичные заявления делаются российскими правоохранительными органами и экспертами[22, 23, 24]. Необходимо отметить, что после освобождения ряда украинских регионов в рамках СВО, с заявлениями о размещении на Украине мошеннических call-центров стали выступать представители правоохранительных органов данных регионов[25].

Появление и деятельность мошеннических call-центров на Украине стала возможной после политических событий 2014 года и разрыва взаимоотношений между правоохранительными органами Украины и РФ. В Уголовном кодексе Украины отсутствует аналог статьи 159.6 УК РФ, поэтому юридически незаконные действия по выводу денежных средств квалифицируются по статье 190 УК Украины («Мошенничество»), где поводом для возбуждения уголовного дела является наличие потерпевшего лица. В случае с украинскими call-центрами потерпевший находится на территории РФ, то есть в недосягаемости для украинских правоохранительных органов, поэтому все call-центры принципиально не работают по гражданам Украины.

Обращают на себя внимание и такие факторы, как экономический и политический кризисы на Украине, повлекшие за собой снижение уровня жизни населения, рост преступности и высокий уровень коррупции. Так, в апреле 2017 года международная аудиторская компания «Ernst & Young» поставила Украину на первое место в мире по уровню коррупции среди 41 исследуемых стран (в том числе стран Африки)[26].

Из комментариев официальных ли[27] и СМИ[28, 29] следует, что деятельностью call-центров управляют организованные преступные группы, а контроль и поддержку им оказывают региональные управления СБУ, включая

---

[22] https://www.mk.ru/social/2021/04/15/telefonnoe-moshennichestvo-v-cifrakh-skolko-aferisty-zarabatyvayut-na-obmane-rossiyan.html

[23] https://aif.ru/society/safety/ohota_na_rossiyan_kak_ukraina_prevratilas_v_fabriku_telefonnyh_moshennikov

[24] https://mvdmedia.ru/news/official/mvd-rossii-prizyvaet-grazhdan-byt-bditelnymi-i-ne-pozvolyat-vovlech-sebya-v-protivopravnuyu-deyateln/

[25] https://tass.ru/obschestvo/15160439

[26] https://web.archive.org/web/20171012070616/https://fraudsurveys.ey.com/ey-emeia-fraud-survey-2017/detailed-results/corruption-perception-by-country/

[27] https://tass.ru/obschestvo/15160439

[28] https://www.1tv.ru/news/2022-04-15/426504-posle_nachala_spetsoperatsii_na_ukraine_v_rossii_rezko_sokratilos_kolichestvo_zvonkov_ot_telefonnyh_moshennikov

[29] https://general-ivanov1.livejournal.com/1088725.html

олигархические кланы. В частности, в марте 2014 года губернатором Днепропетровской области стал И. Коломойский[30], который считается на Украине одним из основоположников деятельности мошеннических call-центров, изначально созданных в г. Днепр и позднее распространившихся по всей Украине. В советское время город - флагман оборонной и космической промышленности, сегодня – непризнанная столица телефонного мошенничества.

На похищенные денежные средства преступники скупают недвижимость внутри страны и заграницей, открывают легальный бизнес, а также финансируют украинские вооруженные силы[31]. Так, по данным Сбера, все чаще мошенники, успешно обманув свою жертву, добавляют в конце разговора «благодарность» за финансирование ВСУ.

1.3. Днепр – центр телефонного мошенничества

В Днепропетровской области действуют более сотни call-центров[32], под которые арендуется большинство офисных площадок, а также частные дома. Количество сотрудников может варьироваться от 10 до 150 человек. В этой криминальной сфере занято около 30% населения в возрасте от 14 до 35 лет[33]. Максимальное количество действующих мошеннических call-центров в г. Днепр достигало 1100, однако, в последнее время оно сократилось до 150: остались только крупные центры, нередко объединенные в сеть[34]. Из каждого украденного мошенниками миллиарда рублей, 650 млн. будут украдены именно мошенническими call-центрами, принадлежащими Днепропетровским ОПГ.

Для осуществления телефонных звонков сотрудниками мошеннического call-центра в качестве потенциальных жертв выбираются граждане РФ, русскоязычные граждане Германии и Израиля, Турции (используются операторы – этнические азербайджанцы), Польши (операторы – бывшие трудовые мигранты), арабских стран (операторы – студенты-граждане арабских государств из многочисленных днепровских ВУЗов). После начала спецоперации на Донбассе зафиксированы попытки атаковать клиентов

---

[30] https://zavtra.ru/events/ukrainskie_koll-tcentri_snova_rabotayut_zhitelyam_rf_opyat_zvonyat_moshenniki_(sotrudniki_bankov)

[31] https://tass.ru/obschestvo/15160439

[32] См. сноску 34.

[33] Одной из причин, по которой г. Днепр стал «столицей» мошеннических КЦ, стало наличие большого количества русскоязычной молодежи.

[34] https://www.rbc.ru/finances/03/10/2021/6158c8299a7947f45b274e7f

европейских банков – граждан стран Евросоюза [35] . При этом, для злоумышленников РФ остается основным источником незаконного обогащения.

На сегодняшний день[36] в г. Днепр свои call-центры есть у представителей всех ОПГ города и Днепропетровского региона: изначально их курировали более молодые члены ОПГ, некоторые ОПГ далее отказывались от участия в наркобизнесе или общеуголовных преступлениях и концентрировались только на деятельности call-центров из-за сверхприбыльности последних. Можно выделить наиболее крупные ОПГ – «Девятки» и «Кошляка»:

ОПГ «Девятки»[37] – благодаря call-центрам преступники за несколько лет прошли путь от группы молодых квартирных воров (1993-94 года рождения) до мультимиллионеров, влияющих на целые отрасли городской экономики. ОПГ сформирована по принципу общности жительства всех участников в одном районе г. Днепр (жил. массив Левобережный и Клочко). В 2015-2018 гг. данная группа занималась квартирными кражами, вымогательствами и другими общеуголовными преступлениями в г. Днепр.

Начало активной работы, связанной с открытием участниками данной ОПГ первых call-центров, датируется концом 2018 года. Благодаря установленным до этого момента тесным коррупционным связям лидера ОПГ Лекишвили Зураба («Зурика»), call-центры группы не подвергались проверке со стороны украинских правоохранительных органов.

[35] https://www.theguardian.com/world/2022/jul/12/europol-phone-scam-defrauding-germans

[36] https://lenta.ru/articles/2017/08/02/dnepropetrovsk/.

[37] https://vklader.com/dnepr-fake-sberbank/.

Рисунок 3. Лидеры ОПГ «Девяток»

Данная ОПГ стала лидером региона среди других сетей мошеннических call-центров благодаря следующим особенностям:

- постоянное изменение схем мошенничества с банковскими картами: от банального получения доступа к конфиденциальным данным кредитных карт (CVV и срок действия карты) и оформления кредитов на потерпевших через онлайн-кабинеты до проведения целых психологических операций над потерпевшими на протяжении нескольких дней и недель, в результате которых потерпевший лично пополняет счета мошенников через банковские терминалы (не только имеющимися наличными, но и кредитными средствами), а в отдельных случаях они вынуждали потерпевших продавать имущество и вносить вырученные средства на счета мошенников;

- методика работы данной сети – быть на один шаг впереди. Аналитиками данных ОПГ тщательно изучаются способы защиты российских банков и проводится поиск слабых мест в выстраиваемой защите банков;

- все call-центры сети работают исключительно по гражданам и банкам РФ, принципиально запрещено работать не только по гражданам Украины, но и по гражданам Казахстана, Беларуси и Польши во избежание проблем по линии Интерпола;

- покупка дорогостоящих клиентских баз данных: известны случаи, когда данная группировка покупала базы данных, состоящие всего лишь из 10 лиц за 10 тыс. дол. США, но все эти люди были VIP-клиентами банков с многомиллионными счетами и, даже если успехом завершалась работа в отношении всего лишь одного из десяти таких клиентов, это окупало затраты;

- на преступников работают десятки психологов, которые обучают всех сотрудников call-центров основам НЛП и грамотному построению речи. Для этого в г. Днепр существует один так называемый «учебный call-центр» на 250 рабочих мест;

- жестокость группы в защите своих интересов. В случае конфликтных ситуаций с другими ОПГ, «Девятки» без раздумий входят в силовое столкновение, не считаясь с последствиями в виде дальнейших проблем с правоохранительными органами. ОПГ известна жестокостью в расправе над своими сотрудниками, уличенными в хищении денежных средств, или теми, кто перешел на работу к конкурентам без согласования: подобное наказывается нанесением увечий, незаконным лишением свободы, татуировками на лице, нанесенными насильственным образом (слово «Крыса»). Данные факты также не расследуются сотрудниками правоохранительных органов, в том числе из-за коррумпированности последних;

- данная преступная группа в своей деятельности придерживается правила «закрыть вопрос» со всеми правоохранительными органами на местном и центральном уровнях, чтобы гарантированно уйти от уголовной ответственности.

ОПГ «Кошляка» известна как одна из самых мощных и многочисленных преступных групп Днепропетровской области. Она насчитывает более 100 участников. Лидером преступной группы является «бизнесмен и меценат», Президент Федерации Дзюдо Украины, депутат Днепропетровского областного совета и основатель благотворительного Фонда «Мироздание» Кошляк Михаил Анатольевич. В 2018-19 гг., путем передела рынка, зачастую включая кровавые разборки и убийства, ОПГ «Кошляка» достаточно быстро стала вторым по численности и качеству игроком на рынке.

Call-центрам «Кошляка» характерно жестокое отношение к сотрудникам со стороны членов ОПГ. «Холоднозвонящие» и «клоузеры» могут быть в любой момент избиты на глазах своих «коллег» за малейшую повинность,

например, за «сорвавшегося» клиента или неправильно подобранного слова, опоздание, появление на работе в состоянии алкогольного или наркотического опьянения. Также членами преступной группы жестоко караются сотрудники, которые переходят на работу в другие «сетки» call-центров.

Организация работы call-центров, работающих под покровительством ОПГ, выглядит следующим образом. Все call-центры, входящие в сеть, делятся на те, которые непосредственно принадлежат членам ОПГ и те, которые работают под так называемой «франшизой» (обычно это группа рядовых сотрудников численностью от 10 человек, которая изъявляет желание работать вместе с ОПГ). Преступники обучают сотрудников будущей «франшизы» своим схемам работы, помогают с запуском call-центра и, соответственно, уведомляют правоохранительные органы о «запуске» нового call-центра во избежание потенциальных проблем.

Распределение дохода мошеннических call-центров происходит следующим образом - 20% средств, выведенных со счета или карты российского банка, забирают сервисы обналичивания украденных средств. Из оставшихся 80% вычитается затратная часть: покупка баз данных, аренда офиса, коммунальные платежи, коррупционная рента. От оставшейся суммы 15% уходят на зарплаты рядовым сотрудникам. Если call-центр принадлежит только членам преступной группы, то прибыль разделяется между всеми лидерами в равных долях. В случае с «франшизой» прибыль делится 50/50 между лидерами ОПГ и хозяевами call-центра, открытого по «франшизе».

Стать партнерами преступников может любой, кто смог собрать устойчивый коллектив и вложиться 50/50 с ОПГ в будущий call-центр. В партнеры не принимают людей, которые имеют отношение к деятельности правоохранительных органов или распространению наркотических средств. Собеседование с кандидатом в партнеры проводит один из лидеров ОПГ.

1.4. Распространение мошеннических call-центров по территории Украины

Телефонное мошенничество по всей территории Украины организовано по примеру днепропетровских call-центров. В настоящее время данный «бизнес» функционирует по модели франчайзинга – организаторы предлагают приобрести call-центр «под ключ», включая сценарии диалога с жертвой, процессы работы, обеспечение актуальными персональными данными, инструменты IP-телефонии, подмены номера и прочее.

В среднем стоимость открытия call-центра на 10-15 сотрудников составляет 5 тыс. долларов США. При этом 3 тыс. долларов США – средняя ежемесячная «такса» за неприкосновенность со стороны сотрудников правоохранительных органов call-центра численностью в 50 сотрудников. Анализ объявлений на сайтах поиска работы на Украине показывает, что по состоянию на конец 2021 г. основная часть call-центров располагается в г. Днепр, чуть меньше – в таких городах, как Запорожье, Каменское, Кривой Рог, Одесса, Киев, Львов, Ивано-Франковск и Бердянск. После начала специальной военной операции на Донбассе часть мошеннических call-центров мигрировала из г. Бердянск и Харьков на запад Украины, в г. Киев, Тернополь и Винницу, и это далеко не исчерпывающий список.

Рисунок 4. Мошеннические call-центры на территории Украины

Об открытости такого криминального бизнеса на Украине можно судить по объявлениям на подбор сотрудников в call-центры. При анализе основных сервисов поиска работы на территории Украины, в том числе по размещению онлайн объявлений в сети Интернет: «Rabota.ua», «Olx.ua», «Work.ua» и даже социальную сеть «Instagram»[38] (рисунки 5-8), нашлись десятки подобных объявлений.

[38] Принадлежит Meta, запрещена в РФ.

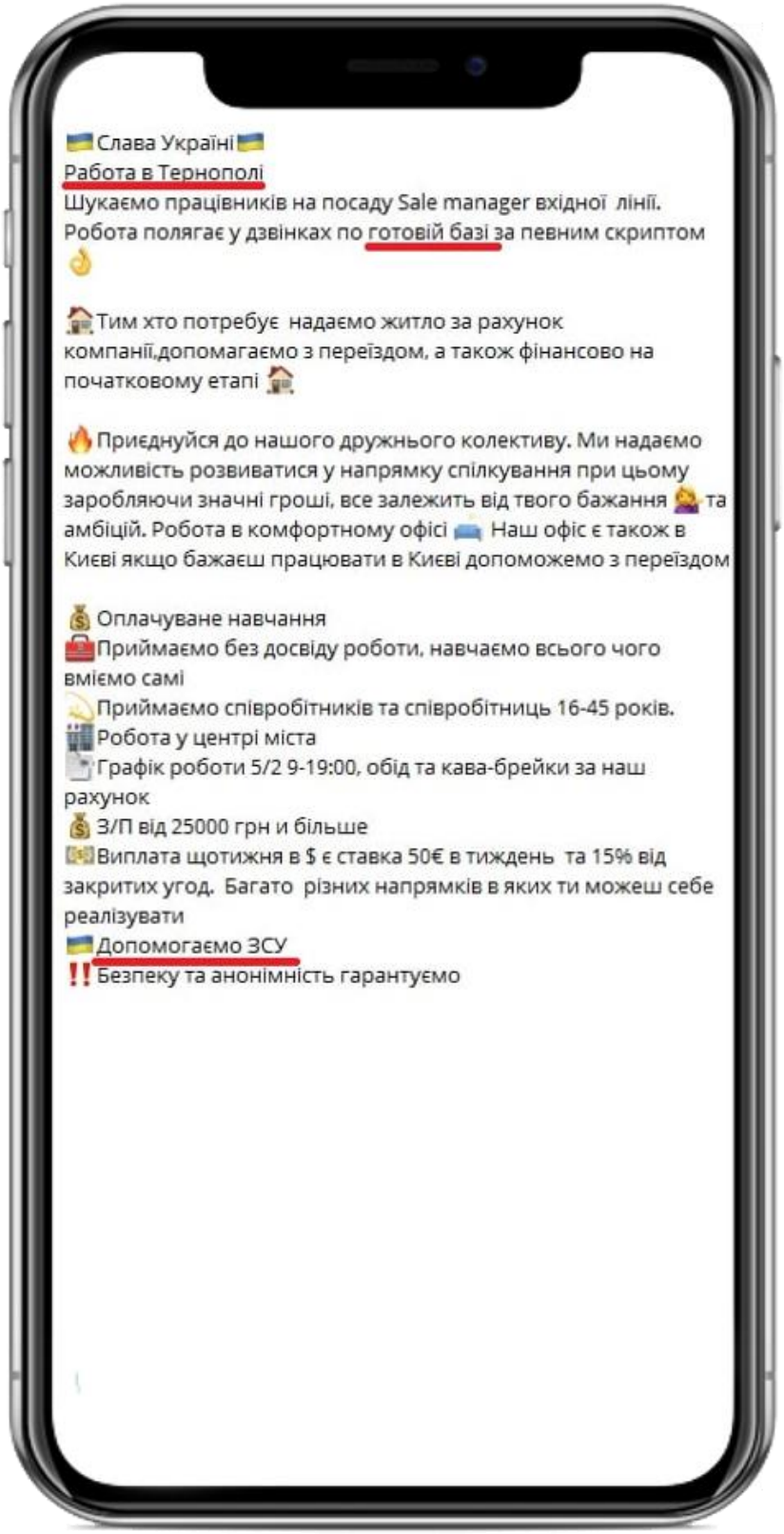


Рисунок 5. Пример объявления набора операторов в call-центр

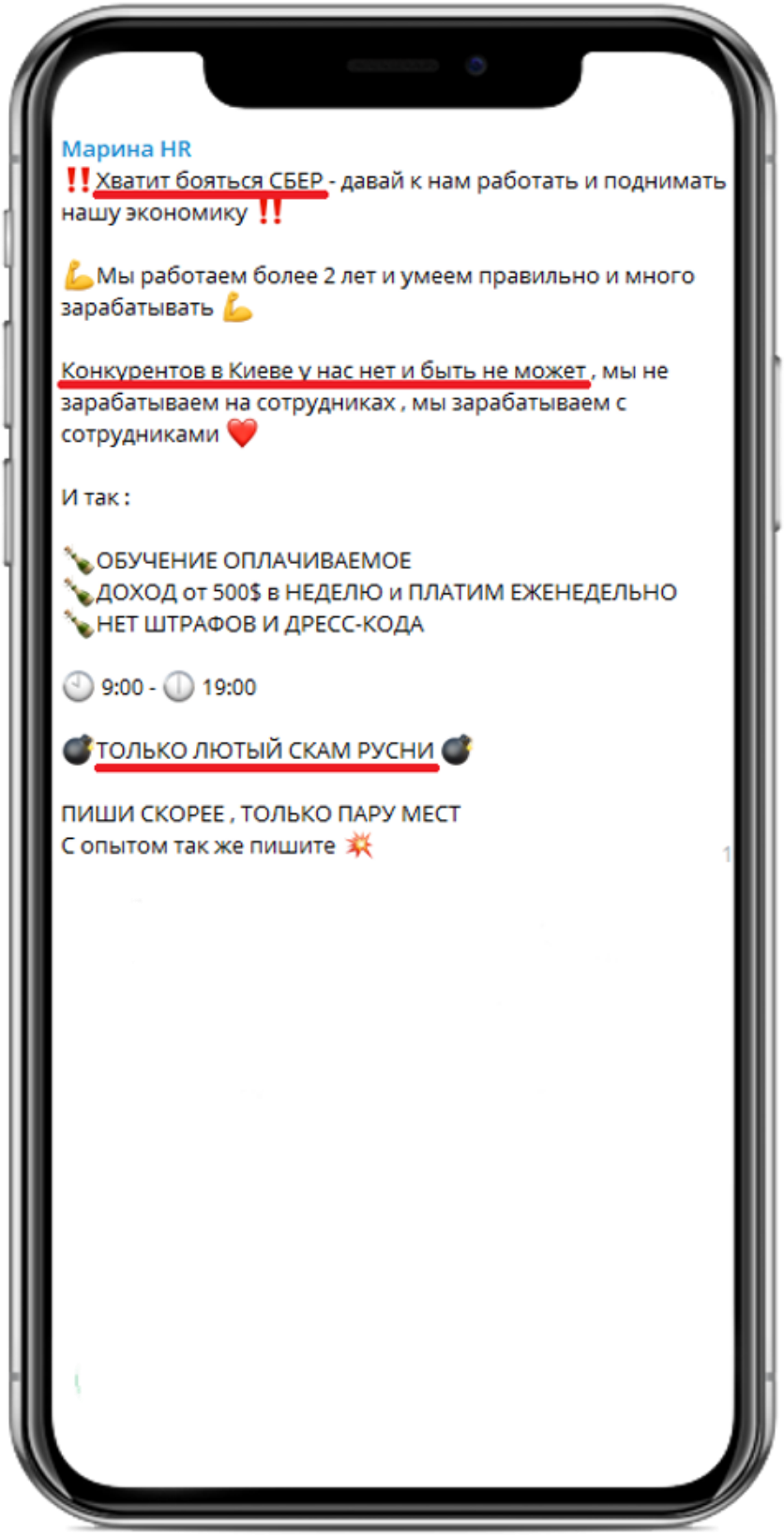


Рисунок 6. Пример объявления набора операторов в call-центр

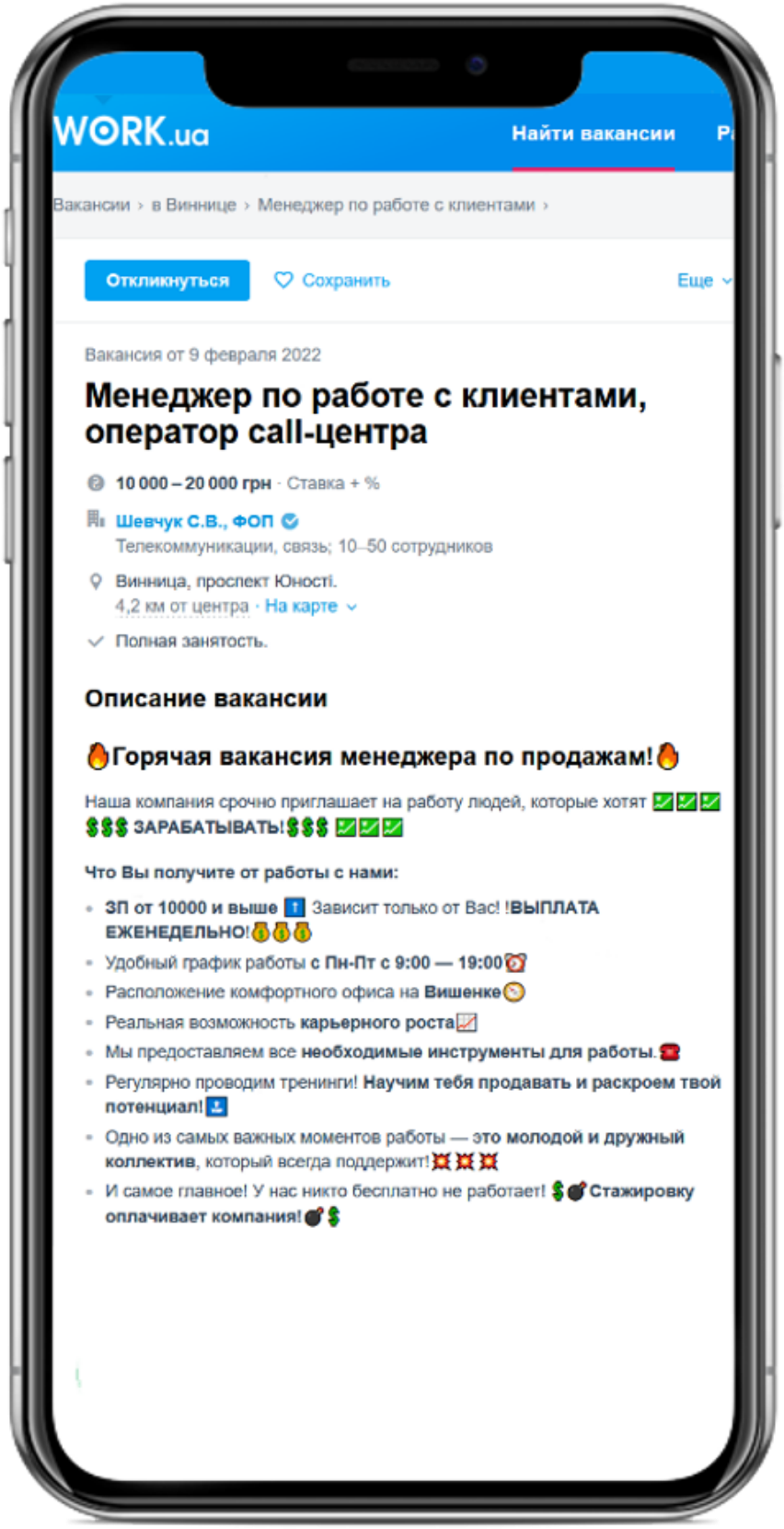


Рисунок 7. Пример объявления в сети Интернет на сайтах с поиском работы

Рисунок 8. Пример аккаунта по поиску сотрудников в call-центры в соцсети Instagram

К характерным признакам данных объявлений можно отнести достаточно высокую заработную плату 10-40 тыс. гривен (25-100 тыс. руб. в неделю). На работу нанимают, как правило, молодых людей до 35 лет, с навыками работы в коллективе, активно пользующихся ПК, с хорошо поставленной речью. Если рекрутеру удается привлечь работника без характерного южнорусского или украинского акцента, то это считается большой удачей, потому что заработки такого сотрудника на порядок выше, чем у сотрудников с акцентом.

На первое время работникам предоставляется оплачиваемое жилье – хостел, который, как правило, находится рядом с call-центром в пешей доступности. Связь с кандидатом по вакансии обычно происходит через мессенджер «Telegram», где обговариваются условия работы, первоначальная ставка по заработной плате и другие особенности (не скрывают, что работают по клиентам российских банков).

Во время первого разговора с кандидатом наниматель из call-центра просит перезвонить с украинского номера телефона, а особенности вакансии стараются обсуждать только лично при встрече. Также требуют предоставить скан украинского паспорта для «проверки» кандидата перед собеседованием, что связано с репортажем о работе телефонных мошенников на Украине (телеканал Россия, «Андрей Малахов. Прямой эфир»), когда корреспондент устроился на работу в call-центр в рамках журналистского расследования.

Место встречи, в большинстве случаев, назначают в непосредственной близости с call-центром. После общения и уточнения всех особенностей работы, если кандидат подходит, его приглашают непосредственно в офис. Кандидата уверяют, что с правоохранительными органами «все подвязано». Все собеседования, как правило, проходят в несколько этапов, что также обеспечивает конфиденциальность работы сотрудников данного call-центра. Средняя заработная плата новичка составляет 200-500 долларов в неделю, а заработок опытного «сотрудника» может составлять 500-2000 долларов.

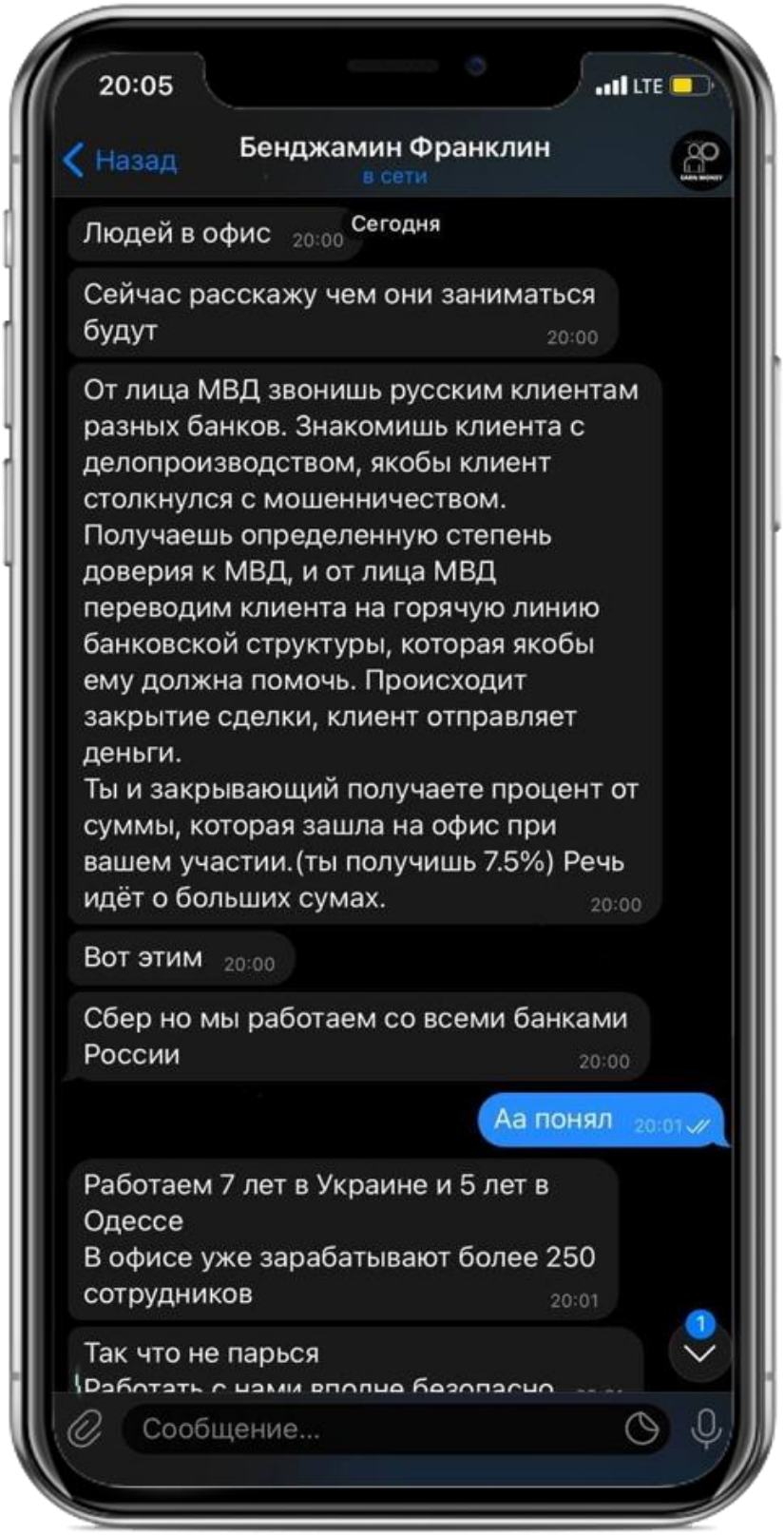


Рисунок 9. Переписка в Телеграм от лица «кандидата» на работу в мошеннический КЦ

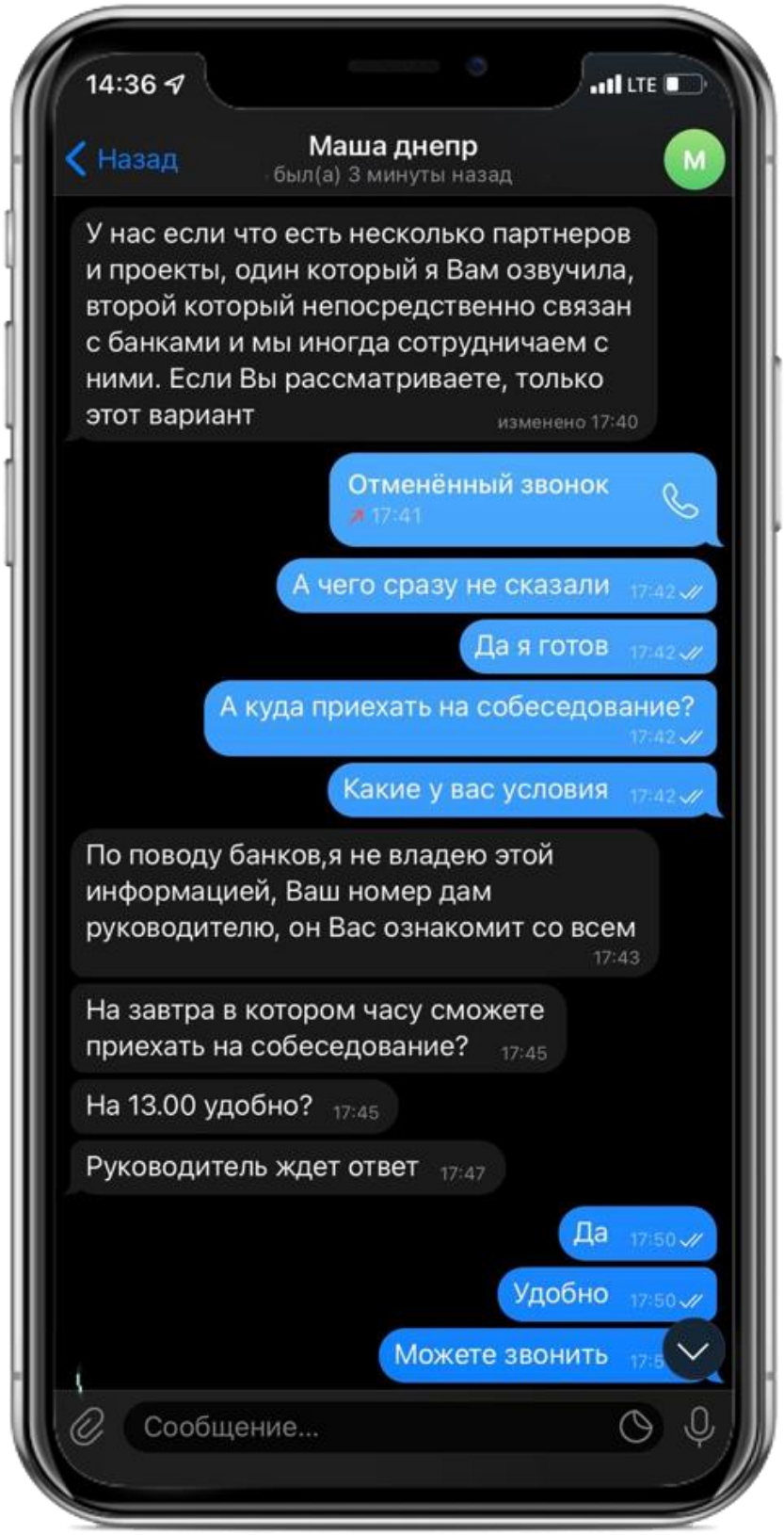


Рисунок 10. Переписка в Телеграм от лица «кандидата» на работу в мошеннический КЦ

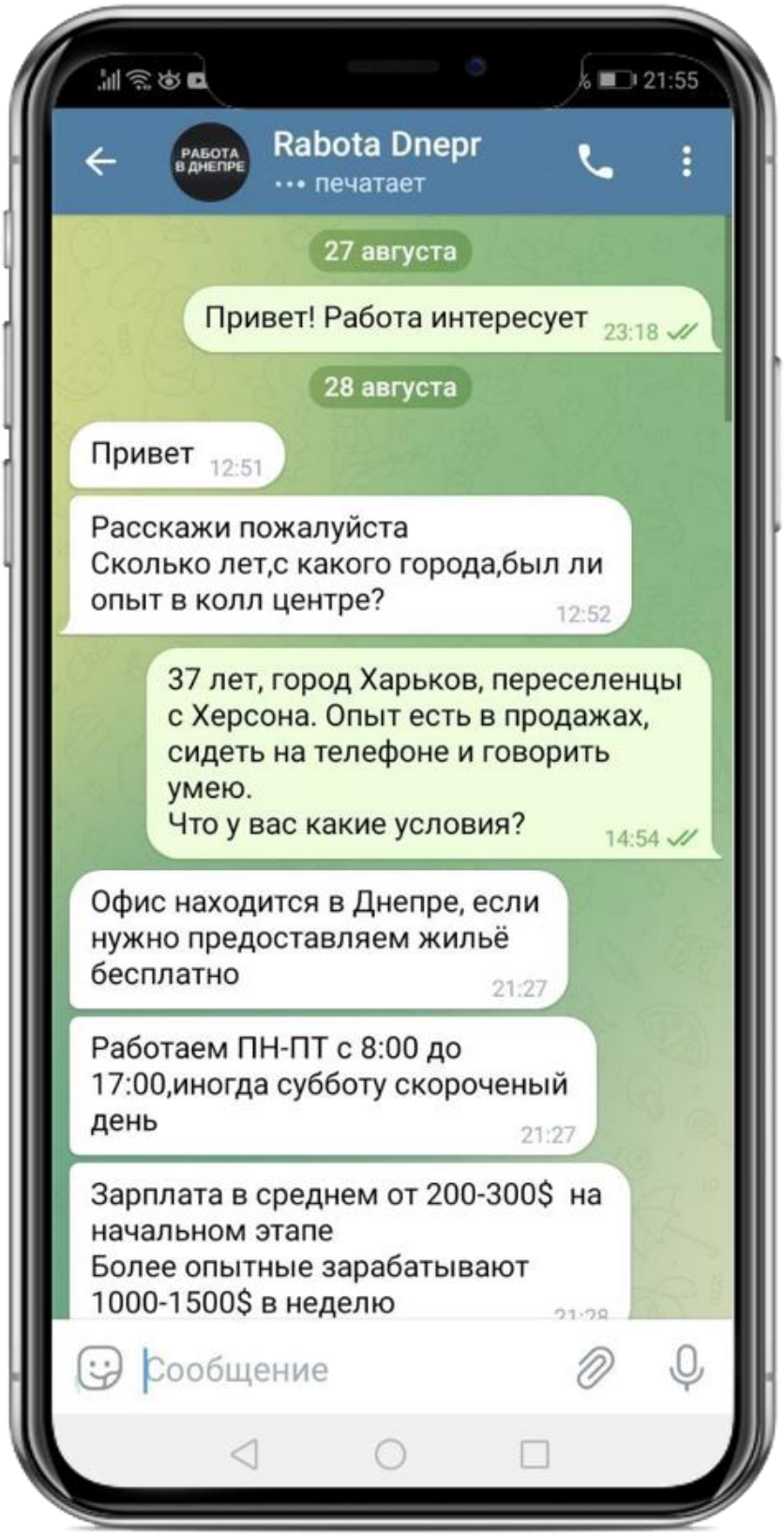


Рисунок 11. Раскрытие деталей работы одного из мошеннических call-центров по переписке с HR-рекрутером мошеннического call-центра

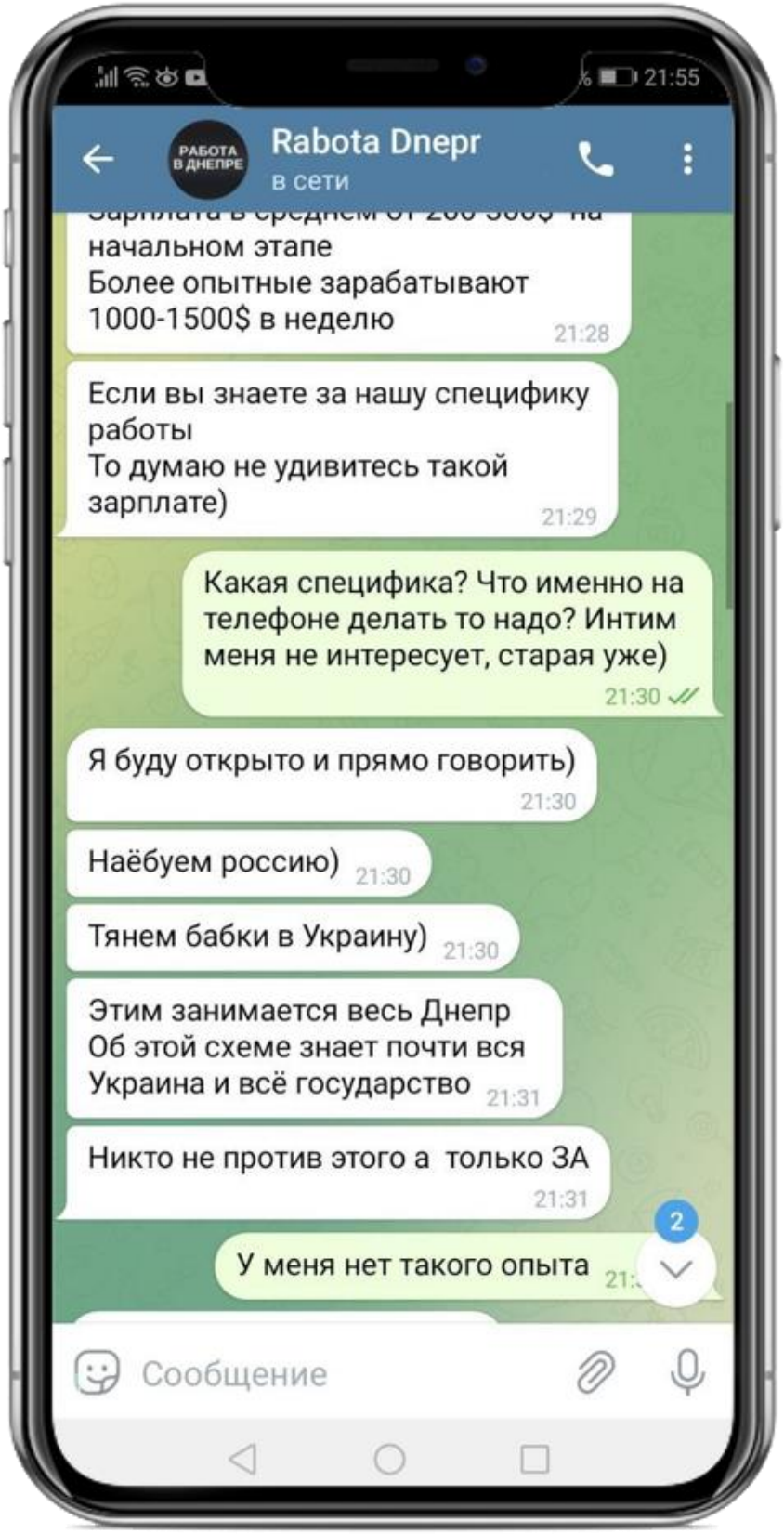


Рисунок 12. Раскрытие деталей работы одного из мошеннических call-центров по переписке с HR-рекрутером мошеннического call-центра

1.5. Организация мошенничества на примере call-центра в г. Бердянск

На протяжении многих лет внутреннее устройство и организация деятельности call-центра была вне зоны досягаемости правоохранительных органов. Однако, в ходе проведения специальной военной операции на Донбассе в середине апреля 2022г.[39], сотрудниками ФСВНГ Росгвардии было обнаружено пустующее помещение, оснащенное компьютерной техникой и телефонией. Проверка данного помещения показала, что в нем был расположен один из крупнейших мошеннических call-центров Украины.

Экспертами Сбера было проанализировано более 14 Тб информации, собранной с компьютерной техники call-центра, что позволило определить организованную структуру, каналы получения данных о гражданах РФ, сценарии разговора, применяемые технологии и другую информацию, позволяющую оценить работу мошенников. Установлено, что с февраля 2020 года до момента начала СВО сотрудники call-центра вели активную деятельность по хищению денежных средств у граждан РФ. Пик такой активности пришелся на вторую половину 2021 года, когда был полностью налажен рабочий процесс и организованна IT-инфраструктура. Начиная с июля 2021 года сотрудники бердянского call-центра участвовали в совершении серии дистанционных хищений со счетов граждан России. Общая сумма доказанного ущерба превышает 300 млн. руб.

По результатам проведенного исследования предположительно установлено, что данный call-центр относился к большой сети, принадлежащей одному организатору. На это указывает структура call-центра, схемы мошенничества и вывода похищенных денежных средств.

Call-центр располагался в арендованном офисе в г. Бердянск, общей площадью более 100 кв. метров недалеко от центра города в доме 43 по ул. Итальянская, рядом со зданием Управления государственной службы охраны при ГУМВД Украины, Бердянский МО УПО. Внешне офис представлял собой одноэтажное кирпичное неприметное здание, без вывесок, с закрытыми окнами, решетками и оборудованное двумя камерами видеонаблюдения, контролирующими входную зону.

[39] https://tvzvezda.ru/news/2022415259-KxrTx.html

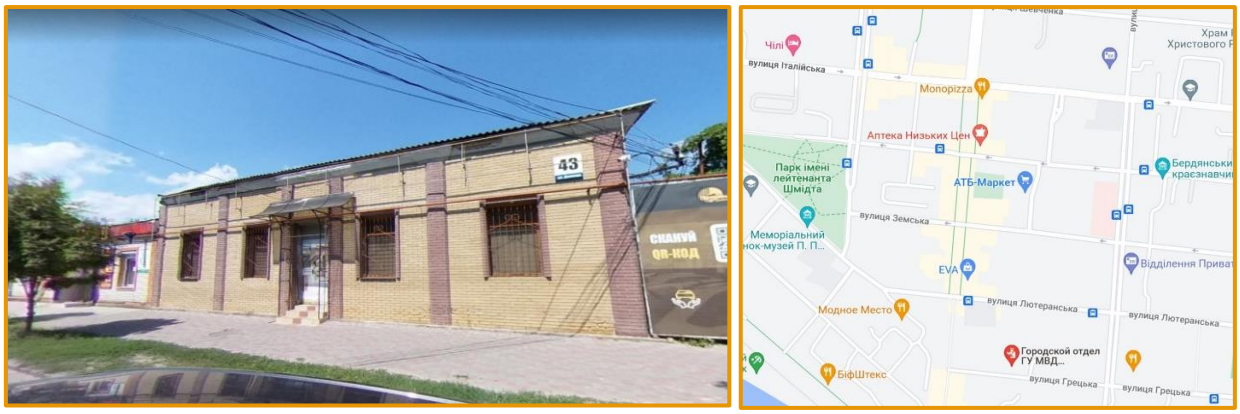


Рисунок 13. Вид здания call-центра снаружи и местоположение на карте

В соседнем здании расположен хостел «Чили», где проживали иногородние сотрудники call-центра. Также рядом с офисом расположены продуктовые магазины, аптеки, ТЦ. Арендная плата составляла в среднем в 20-25 тыс. гривен/месяц (52 тыс. рублей), что на фоне доходов представляет минимальные затраты.

Характерно, что внутри офиса на одной из стен была обнаружена свастика. В самом офисе расположено порядка 70 рабочих мест: персональные компьютеры с гарнитурой, счетчики купюр, сейф для хранения наличных денежных средств, шредер для уничтожения документов.

Рисунок 14. Кадры видеосюжета о ликвидации call-центра в г. Бердянске, СМИ

Установлено, что в call-центре работало до 300 сотрудников в сменном режиме, совершавших около 5 тыс. звонков в сутки. Основной объем звонков приходился на клиентов ВТБ, Альфа-банка, реже Сбера. Для обмана граждан использовалось более 150 различных скриптов разговора, также были обнаружены отдельные методички по работе со «сложными клиентами» и отработке вопросов и возражений.

В результате анализа информации из ПК данного call-центра экспертами Сбера было идентифицировано значительное число его сотрудников и получена информация, позволяющая судить о масштабах его деятельности, связях с криминальными структурами и государственными органами Украины. Количество установленных пострадавших превышает несколько тысяч граждан РФ. Вся информация передана российским правоохранительным органам, проводящим необходимые мероприятия по привлечению преступников к ответственности.

В следующих разделах мы подробнее расскажем о деятельности данного call-центра, его организации, способах обмана клиентов российских банков, методах вывода похищенных денежных средств злоумышленниками. Будет рассмотрена организация IT-инфраструктуры call-центра, раскрыты личности некоторых сотрудников и схемы взаимодействия с организаторами.

2. ОРГАНИЗАЦИЯ РАБОТЫ CALL-ЦЕНТРА «БЕРДЯНСК»

2.1. Основные «бизнес-процессы»

«Бизнес-процессы» call-центра включали в себя закупку баз данных потенциальных жертв, подготовку сотрудников, осуществление мошеннических звонков, организацию вывода денежных средств с помощью специальных сервисов. Для поддержки «бизнес-процессов» была создана полноценная инфраструктура, о которой пойдет речь в третьем разделе. Организационная структура call-центра представлена на рисунке 15.

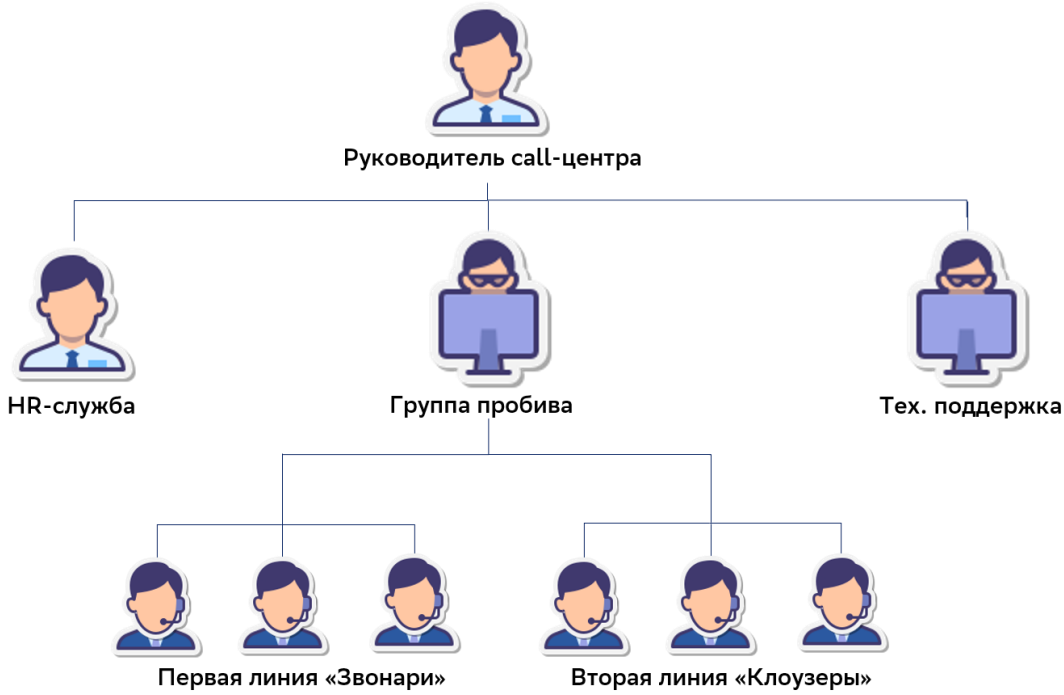


Рисунок 15. Организационная структура call-центра «Бердянск»

Наиболее многочисленными были сотрудники call-центра, выполняющие функции обзвона потенциальных жертв. Установлено, что эти сотрудники были разделены на несколько групп примерно по 30 человек, в зависимости от функциональных задач:

- 1-я линия обзвона, т.н. «звонари» – наименее квалифицированные сотрудники, которые совершают звонки по заранее заданному скрипту и ищут клиентов, подверженных воздействию. Затем жертву передают на вторую линию.
- 2-я линия обзвона, т.н. «клоузеры» – термин, который пришел из области продаж. Данным термином (от англ. глагола «to close», закрывать) называют сотрудников, завершающих или «закрывающих» деловую сделку. В мошеннических call-центрах сотрудникам с данной ролью доверяют «закрыть» клиента. Как правило, клоузером становится наиболее опытный специалист с отработанными навыками продаж и убеждения. Он может

представляться управляющим банка, сотрудником МВД или ФСБ России – это позволяет злоумышленникам создавать иллюзию, что клиент столкнулся с серьезной проблемой, связанной якобы с «внутренним мошенничеством», ему угрожают потерей денежных средств, но если он пойдет на сотрудничество и будет выполнять инструкции, то ущерба удастся избежать.

Также были выявлены лица, выполнявшие сопровождающие функции:

- группа технической поддержки;
- группа поиска баз данных для обзвона;
- группа обогащения имеющихся персональных данных гражан РФ через специализированные Интернет-сервисы (т.н. «пробива» данных).

Для организации работы групп использовались Telegram-чаты с нескольким набором имен: «murka XX», «kontora777 XX» (где XX порядковый номер). Анализ переписки в чатах позволил установить следующее:

1. «murka XX», 1-я линия (звонари) могут полностью реализовывать мошенническую схему без привлечения сотрудников второй линии;
2. «kontora777 XX», 2-я линия (клоузеры). Подключаются к схеме на финальных этапах, «заказывают дропов» на площадке, выводят денежные средства.

Работу ИТ-инфраструктуры call-центра обеспечивали инженеры, осуществлявшие настройку SIP-телефонии на персональных рабочих местах сотрудников, ежедневно рассылали учетные записи SIP-телефонии, оказывали помощь в настройке оборудования и устранении проблем. Для получения помощи необходимо было обратиться в специальную Telegram-группу «Тех. поддержка» (см. рисунок 16 и 17).

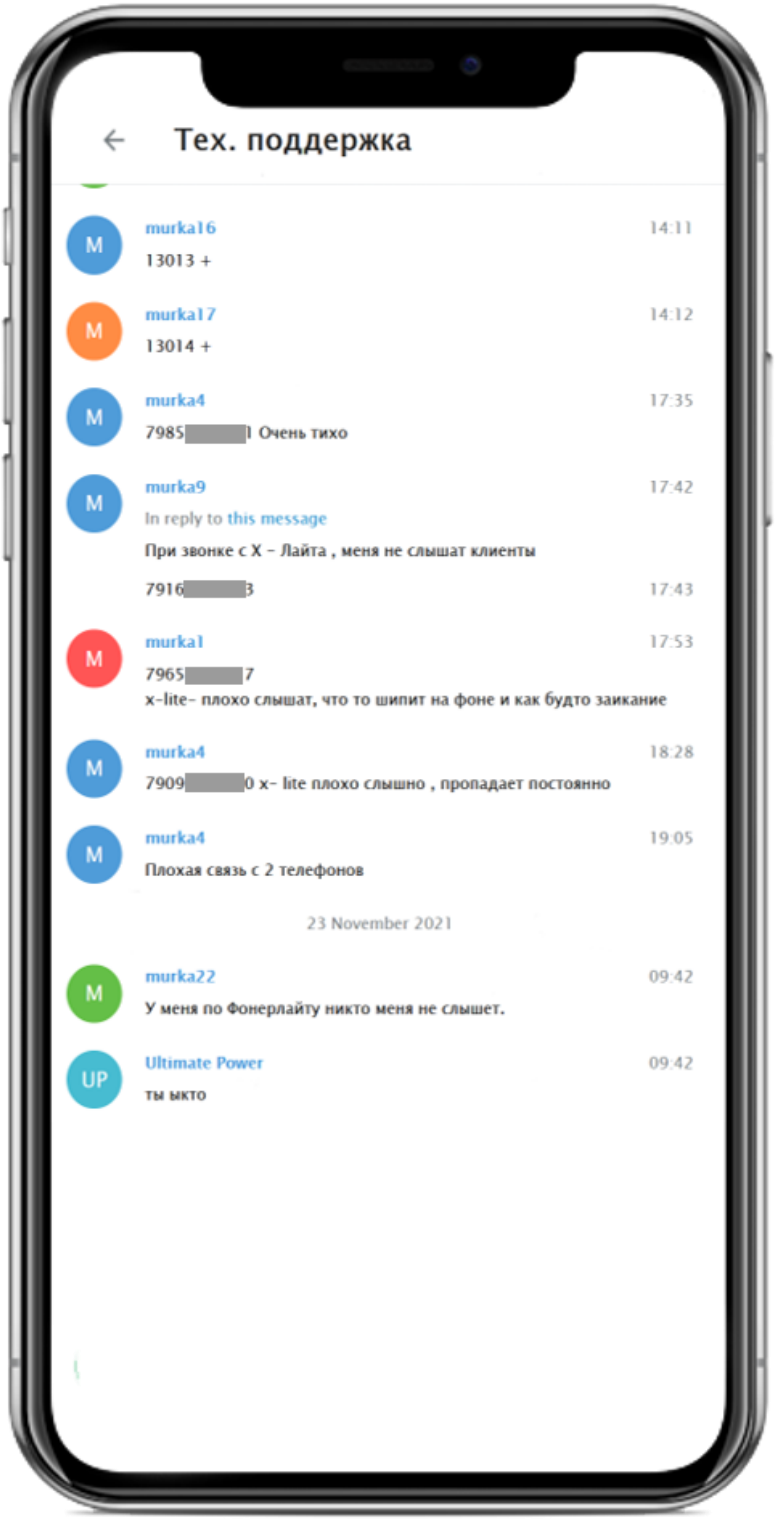


Рисунок 16. Пример 1 переписки «пользователей» с сотрудниками «Тех. поддержки»

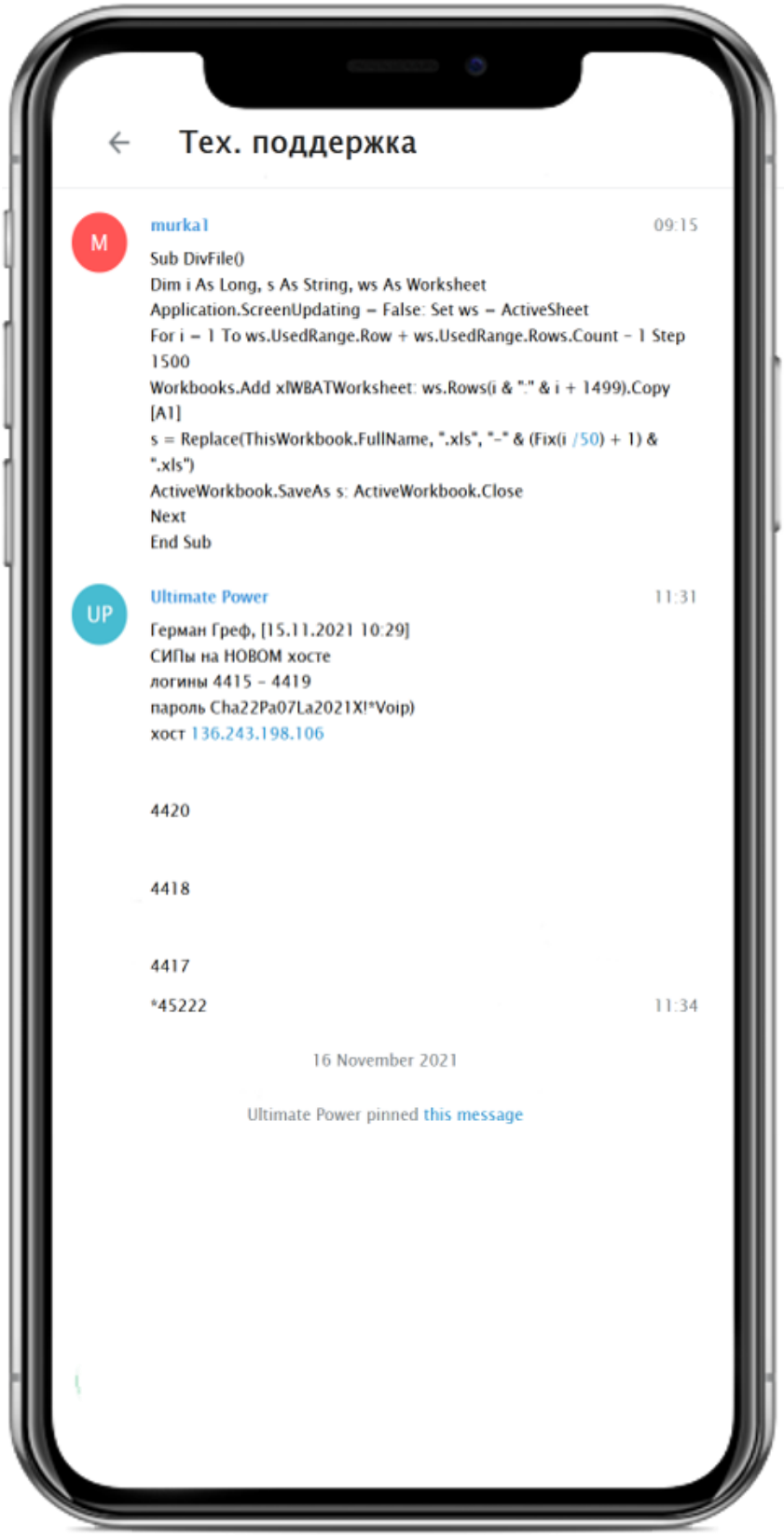


Рисунок 17. Пример 2 переписки «пользователей» с сотрудниками «Тех. поддержки»

Организация работы мошеннической схемы состояла из 4 основных этапов (Рисунок 18).

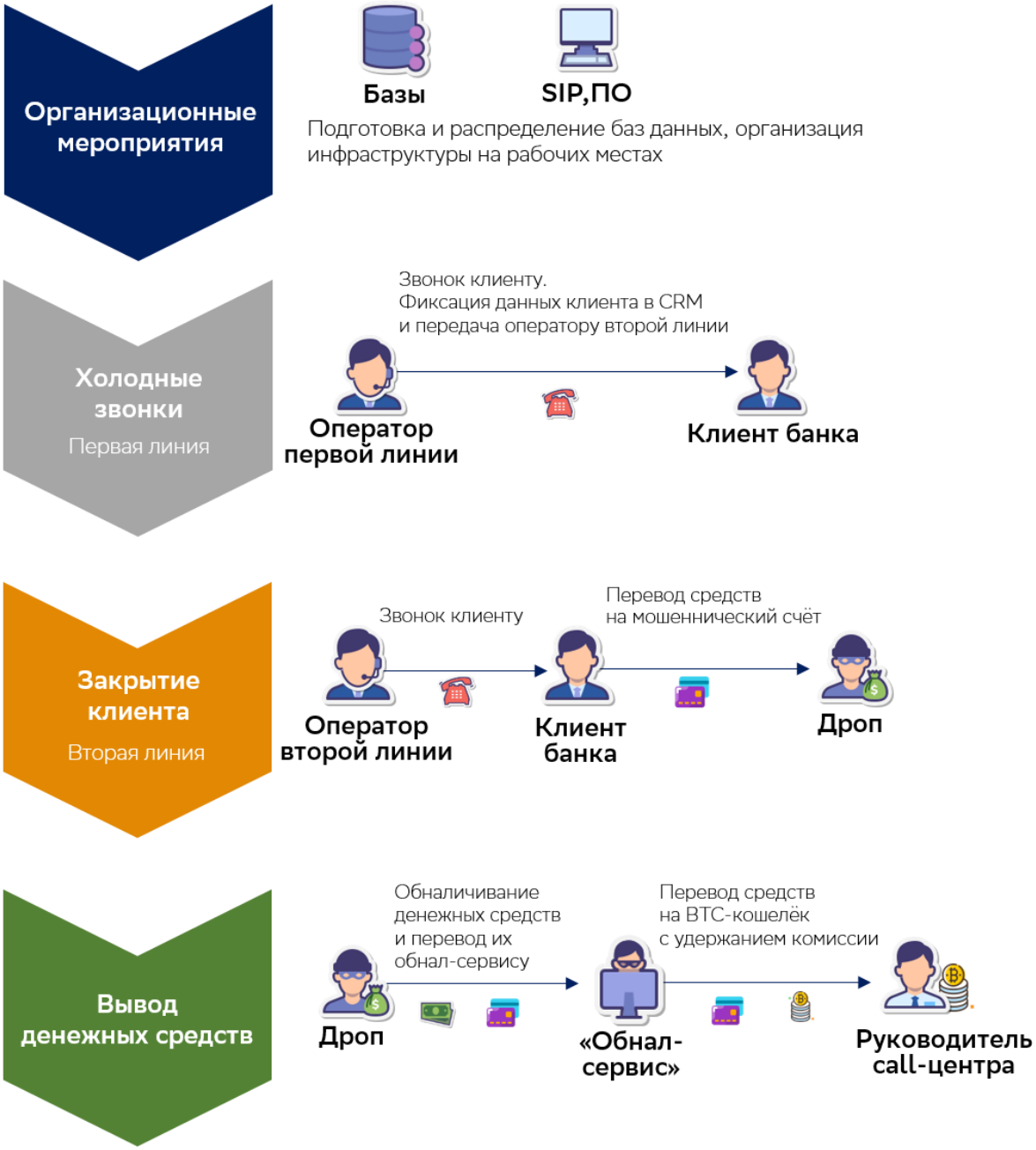


Рисунок 18. Схема организации рабочего процесса

1. **Организационные мероприятия**. Настройка оборудования, SIP-телефонии, подготовка и распределение между сотрудниками баз данных.
2. **Холодный звонок** клиенту. Фиксация информации в CRM и передача клиента на «вторую линию». Оператор вносит полученную во время разговора информацию об операциях, счетах и вкладах клиента в CRM.
3. **«Закрытие» клиента**. Оператор «второй линии» звонит клиенту и, используя информацию, полученную на предыдущем этапе и внесенную в CRM, убеждает клиента совершить перевод на мошеннический счет. Оператор «второй линии» связывается с сервисом «обнала» (т.н. «дроп-

сервис» или «обнал-сервис»), передает информацию о сумме средств для вывода и получает в ответ мошеннические реквизиты (например, номер банковской карты) для вывода украденных денежных средств (т.н. «дроперские» счета).

4. **Вывод денежных средств**. Обнал-сервис организует обналичивание переведенных жертвой средств с дроперского счета, забирает свою комиссию (около 20%), а оставшаяся сумма переводится сервисом на подконтрольные руководителям call-центра BTC-кошельки.

2.2. Сбор данных о жертвах

За сбор данных потенциальных жертв в мошенническом call-центре отвечал выделенный сотрудник, покупавший украденные базы данных в теневом сегменте сети Интернет (даркнет). «Закупщики» использовали специально созданные одноразовые Telegram-аккаунты, удалявшиеся после сделки. Как правило, покупались базы данных мобильных операторов связи, банков, онлайн-магазинов и т.д. Стоимость таких баз данных составляет от 100 до 500 долларов США за 1000 строк. Установлены площадки и продавцы, с которыми работал call-центр, вся информация по ним была передана в правоохранительные органы.

Базы данных распределялись между конкретными сотрудниками, осуществлявшими обзвон. Во избежание повторных звонков жертвам, каждый сотрудник работал по своей базе. Для хранения и обработки данных, полученных от клиента уже во время телефонного разговора, каждый сотрудник вносил информацию по жертве в CRM.

В начале рабочего дня сотрудник, отвечающий за базы данных, рассылал «звонарям» подготовленные файлы с данными для обзвона. Он формировал такие файлы на основе информации из баз данных, приобретенных ранее. Когда «звонарь» заканчивал работу с одним файлом, ему присылали новый в течение дня. Также сотрудники 2-ой линии дополнительно брали у сотрудника, отвечающего за базы данных, файлы на «тест», т.е. проверяли информацию из файлов на актуальность или на факт прозвона по ней со стороны других call-центров (оценка делалась по реакции абонента на звонок).

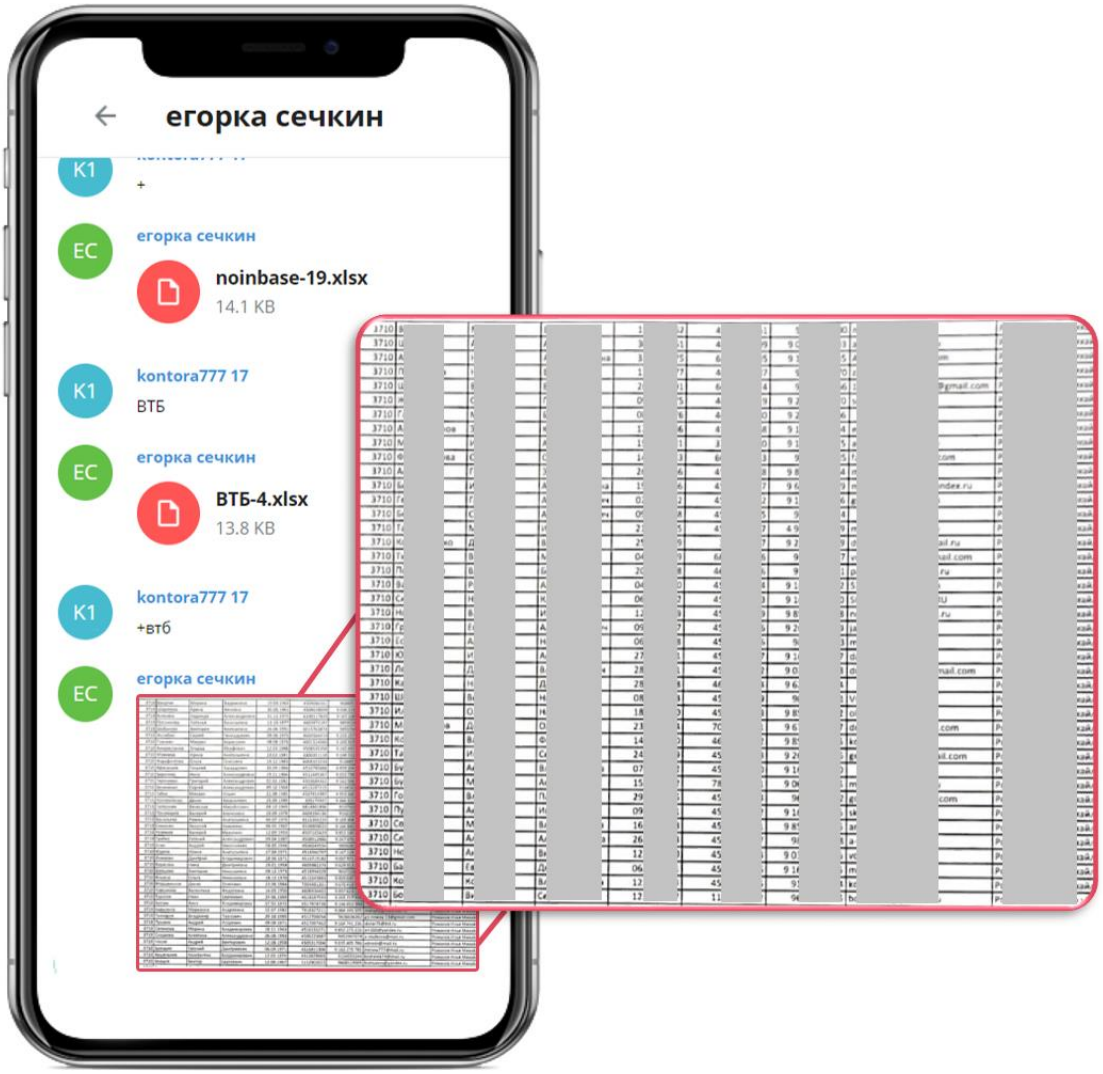


Рисунок 19. Рассылка файлов с информацией о клиентах

Файлы представляли из себя таблицы, содержащие от 50 до 100 записей с ФИО, адресами, номерами телефонов и прочими персональными данными потенциальных жертв. Всего на проанализированных дисках обнаружено более 10 тысяч таких файлов.

Информация в базах данных представляет собой компиляцию из различных утечек (более 30 млн. строк), получивших огласку в СМИ: СДЭК, торговой сети «Красное и Белое», Яндекс.Еда 2021 и др. Отдельно стоит отметить, что значительная часть фрагментов баз данных содержала информацию о клиентах Альфа-Банка и ВТБ, реже Сбера, исходя из чего можно предположить, что имели место таргетированные атаки на клиентов именно этих банков.

Также в ходе исследования были обнаружены многочисленные материалы, содержащие логотипы белорусских банков, а именно: Беларусбанк, Альфа-Банк БелВЭБ, ВТБ (Беларусь), Дабрабыт, Белагропромбанк, Белгазпромбанк,

Белинвестбанк, МТБанк, Национальный банк РБ, Приорбанк, Технобанк (рисунок 20), изображение удостоверения сотрудника правоохранительных органов (рисунок 21), памятки по законодательству и прочее. Данный факт может свидетельствовать о том, что жертвами бердянского call-центра могли быть также и граждане Республики Беларусь.

Рисунок 20. Обнаруженные логотипы Белорусских банков

Рисунок 21. Удостоверение сотрудника Управления Следственного комитета РБ по г. Минску

Если информации в базах данных было недостаточно, то сотрудники группы «пробива клиентов» осуществляли дополнительный сбор сведений о потенциальной жертве. Основным инструментом поиска являлись специализированные Telegram-боты. Такие боты агрегируют информацию из различных баз данных, украденных из организаций, и предоставляют

возможность получить, например, по номеру телефона различную исчерпывающую информацию о его владельце.

Так, через Telegram-бот «Глаз Бога» можно было заказать «расширенный поиск» по требуемому субъекту: найти о нем по номеру телефона дополнительную информацию в социальных сетях и коммерческих сервисах Вконтакте, Skype, Одноклассники, WhatsApp, Telegram, GetContact, NumBuster, TrueCaller, объявления на Avito, Youla, Auto, Cian и пр. Кроме того, сервис позволяет отправить анонимное SMS-сообщение, а за 15 рублей получить образец голоса абонента. При выборе подобной услуги абоненту поступает звонок, определяющий доступность телефона, и в случае, если абонент принял вызов, включается диалог с голосовым роботом. Файл с записью голоса поступает инициатору запроса сразу после завершения диалога, длительность составляет 10 секунд, при этом можно выбрать сценарий звонка – «мужчина», «девушка», «грубый», «наглый», «школьник», «курьер».

Таким образом, имея минимальный набор первичной информации об атакуемом (например, только номер телефона), с помощью специальных Telegram-групп злоумышленники получали исчерпывающую информацию о своей жертве[40] и совершали эффективные адресные атаки на конкретную жертву, создавая у нее ощущение, что с ней действительно разговаривает сотрудник банка или правоохранительных органов. Необходимо отметить, что по данным Сбера, в даркнете действует более 30 разнопрофильных площадок с аудиторией более 2.3 млн. зарегистрированных аккаунтов. Услуги по продаже и «пробиву» данных предоставляют 12 из них.

Поэтому злоумышленникам для совершения атак не требовался широкий набор персональных данных. Фактически им было достаточно только номера телефона, имени и отчества его владельца.

[40] Стоимость подписки на «Глаз Бога» составляет 3500 рублей, «Quick Osint» – 59.99 $ на 1 год пользования. В рамках подписки доступно 100 запросов в сутки, за дополнительную плату можно расширить количество запросов и получить дополнительную информацию.

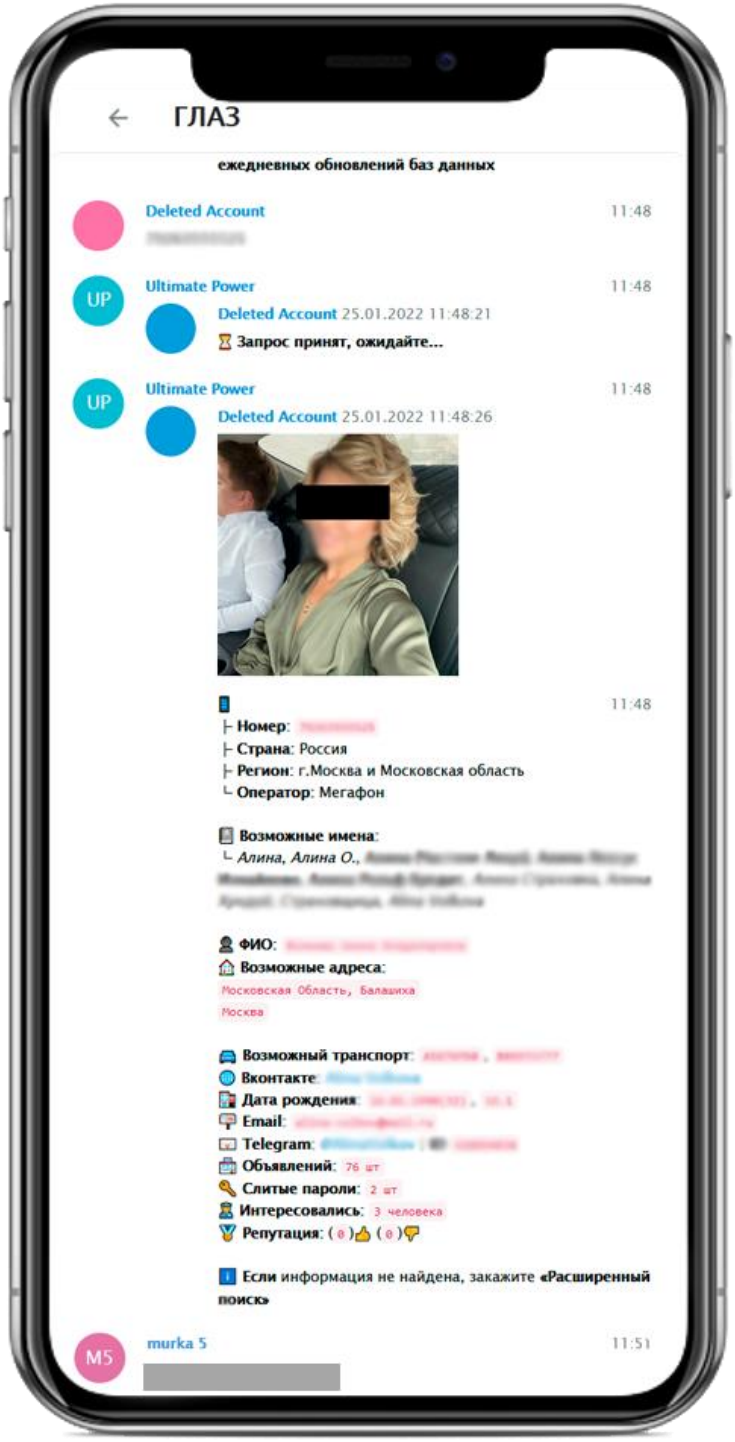


Рисунок 22. Данные клиента, полученные мошенниками через Telegram-группу «Глаз Бога»

2.3. Сценарии обмана

Сотрудниками call-центра осуществлялись звонки по заранее подготовленным сценариям (скриптам). В ходе анализа рабочих мест сотрудников call-центра было обнаружено более 150 таких сценариев (рисунок 23).

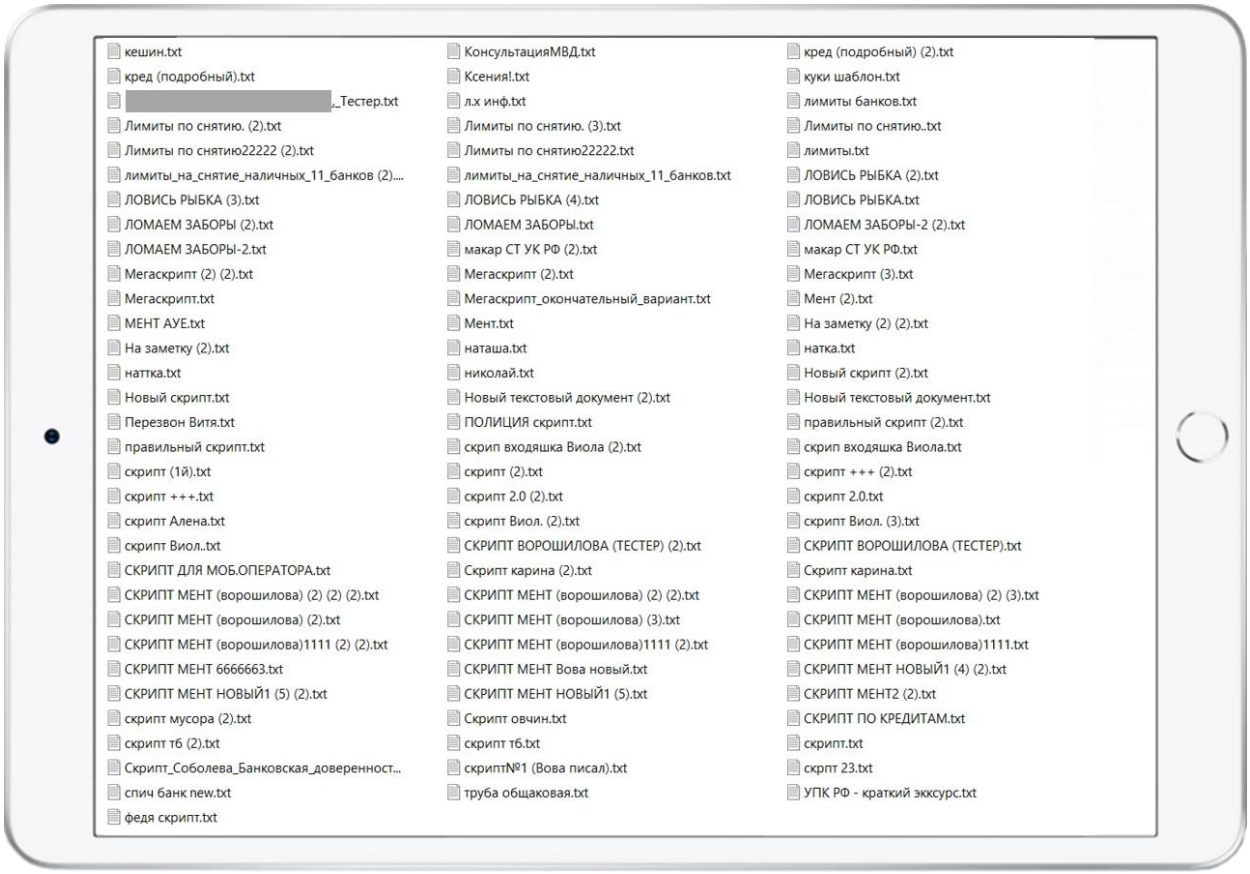


Рисунок 23. Файлы со скриптами

Существовало два основных сценария: звонки от имени службы безопасности банка и звонки от имени правоохранительных органов. Каждый сотрудник, в зависимости от опыта работы, добавлял в скрипт некоторые особенности, помогавшие войти в доверие к клиенту. Обзвонщик представлялся сотрудником того или иного банка в зависимости от информации о клиенте, которой он располагал (рисунок 24).

Рисунок 24. Схема применения скриптов

Основной задачей «холоднозвонящего»[41] сотрудника первой линии обзвона являлось установление контакта с клиентом и получение информации о его счетах, картах и операциях. Как правило, жертве сообщали, что некие злоумышленники якобы завладели данными ее банковской карты (при передаче третьим лицам или при использовании банковской карты в интернет-приложениях). Если жертва шла на контакт, сотрудник «сверял» с ней информацию о ее счетах, вкладах и остатках в различных банках. Информация, полученная от жертвы, фиксировалась в CRM, затем клиент передавался на вторую линию, где «клоузеры» осуществляли списание денежных средств с его счетов, выбирая сценарий вывода средств под конкретный банк, в котором обслуживалась жертва.

Если на счетах жертвы имелась значительная сумма, то мошенники вынуждали ее обналичить средства. Для этого использовались скрипты «Безопасный счет» или «Страховая ячейка»: сценарии, в которых жертву убеждали внести средства наличными якобы на специально созданный для спасения от мошенников «безопасный» счет. В действительности это были мошеннические реквизиты банковских счетов или карт, полученные от дроп-сервиса. Как правило, для взноса средств использовались банкоматы банков, позволяющих вносить средства на счета без дополнительной идентификации вносителя.

При отсутствии значительной суммы у клиента, оператор использовал сценарий «Кредит» и пытался подвести клиента к осуществлению заёма денежных средств в нескольких банках (т.н. «кредитная карусель»). Как правило, у мошенников уже была информация, какие суммы и в каких банках чаще всего оформляются в кредитах без дополнительных проверок со стороны служб безопасности (рисунок 25).

[41] Сотрудник, осуществляющий «холодный» обзвон потенциальных жертв. Холодный звонок – одна из форм телемаркетинга, когда менеджер звонит клиенту, с которым не имел дела ранее.

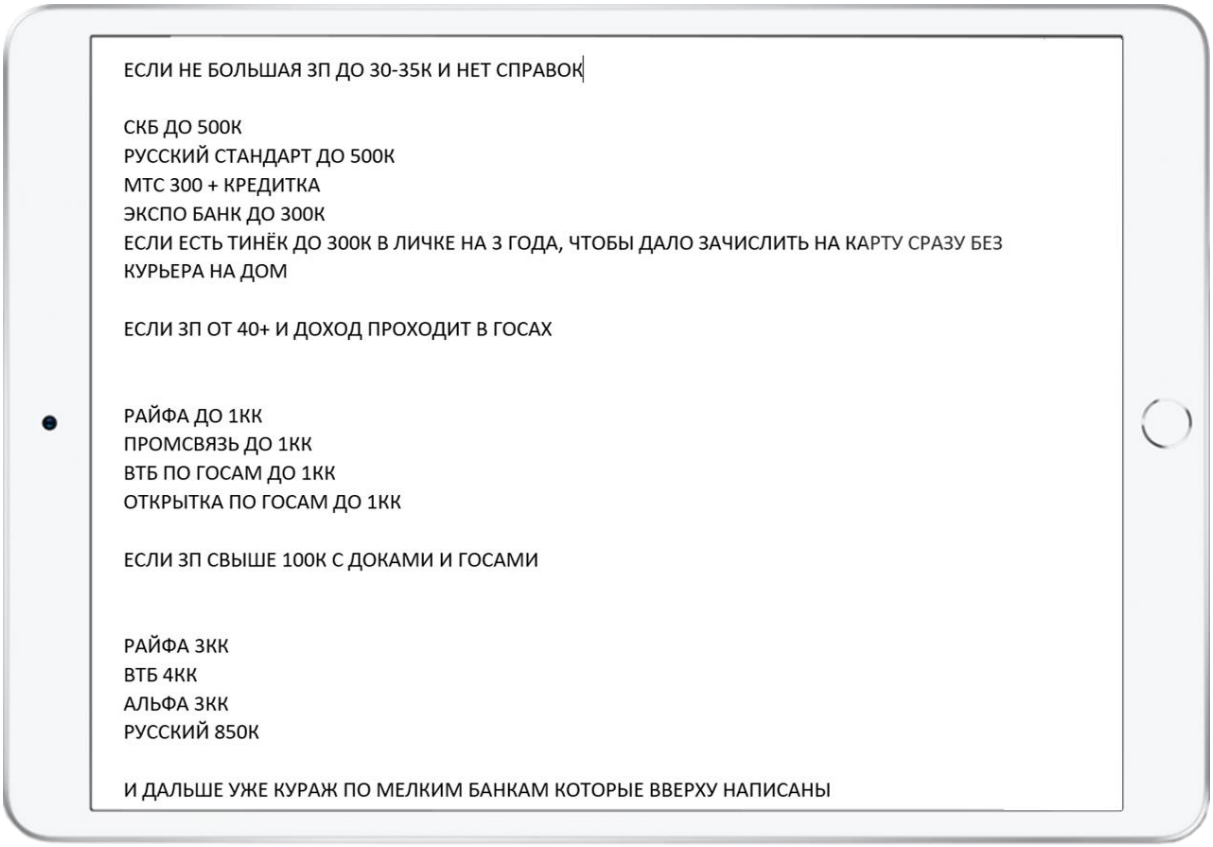


Рисунок 25. Скрипт «Кредит».

Еще одной схемой являлся обзвон будущих жертв от имени сотрудников правоохранительных органов (чаще – следователей). В этом сценарии жертве сообщалось о якобы имеющемся производстве или проверке по уголовному делу по ст. 159 УК РФ («Мошенничество»). Жертве сообщалось, что якобы по заявлению от представителя ЦБ РФ группа лиц использовала лицевой счет клиента для распоряжения денежными средствами, полученными преступным путем. Необходимым условием работы схемы являлось сохранение жертвой данного разговора в тайне (клиенту разъяснялось, что разглашать данную информацию нельзя даже близким родственникам). В дальнейшем клиента передавали на вторую линию и в разговор вступал «сотрудник ЦБ РФ», который подтверждал информацию о «мошенниках» и клиенту предлагалось перевести собственные или заемные денежные средства на «безопасный счет».

Для сомневающихся клиентов существовал специально разработанный скрипт «ломаем заборы», в котором описывалось какими терминами должны оперировать сотрудники call-центра и как строить разговор, если клиент усомнился в правдоподобности звонка: мошенники убеждали клиентов, что звонки банка могут быть не только с короткого номера «900», но и с других номеров «с защищенной линии технического отдела службы безопасности». Для убедительности клиенту называлась сумма и время его последних проведенных операций (эту информацию мошенники узнавали от самого

клиента через первую линию). Ниже приведены примеры некоторых ответов на основные вопросы от сомневающихся клиентов:

Мошенник: - Назовите последнюю операцию и остаточный баланс.

Клиент (сопротивление): - Не, я не буду называть, у вас есть эта информация!

Мошенник (работа с сопротивлением): - На данный момент вся информация по вашему лицевому счёту заблокирована по факту мошенничества. Поэтому нам нужно зафиксировать в голосовом порядке ваш актуальный баланс, чтобы в случае дальнейших мошеннических операций банк компенсировал данную разницу в 100% объеме.

Клиент (сопротивление): - Почему вы не звоните мне с номера 900?

Мошенник (работа с сопротивлением): - Номер 900 – это номер call-центра, который не компетентен в вопросах по факту мошенничества, я же связался с вами с защищенной линии технического отдела службы безопасности, которая занимается фактом мошенничества. Все звонки так же контролируются с защищённой линии и не могут быть прослушаны мошенниками.

Мошенник: - Назовите баланс вашего вклада?

Клиент (сопротивление): - Я не помню!

Мошенник (работа с сопротивлением): - Возьмите договор, какая сумма у вас указана? Зайдите в личный кабинет, посмотрите актуальный баланс.

В зависимости от скрипта и хода общения с клиентом, денежные средства могли также похищаться через внесение наличных самим клиентом на счета «дропов» в различных банках, с помощью привязки личного кабинета клиента к телефонам мошенников или используя привязку карт к различным платежным сервисам: например, Google Pay, Мир Pay и другим. (см. рисунки 26, 27). Детально вывод похищенных средств описан в разделе 2.4.

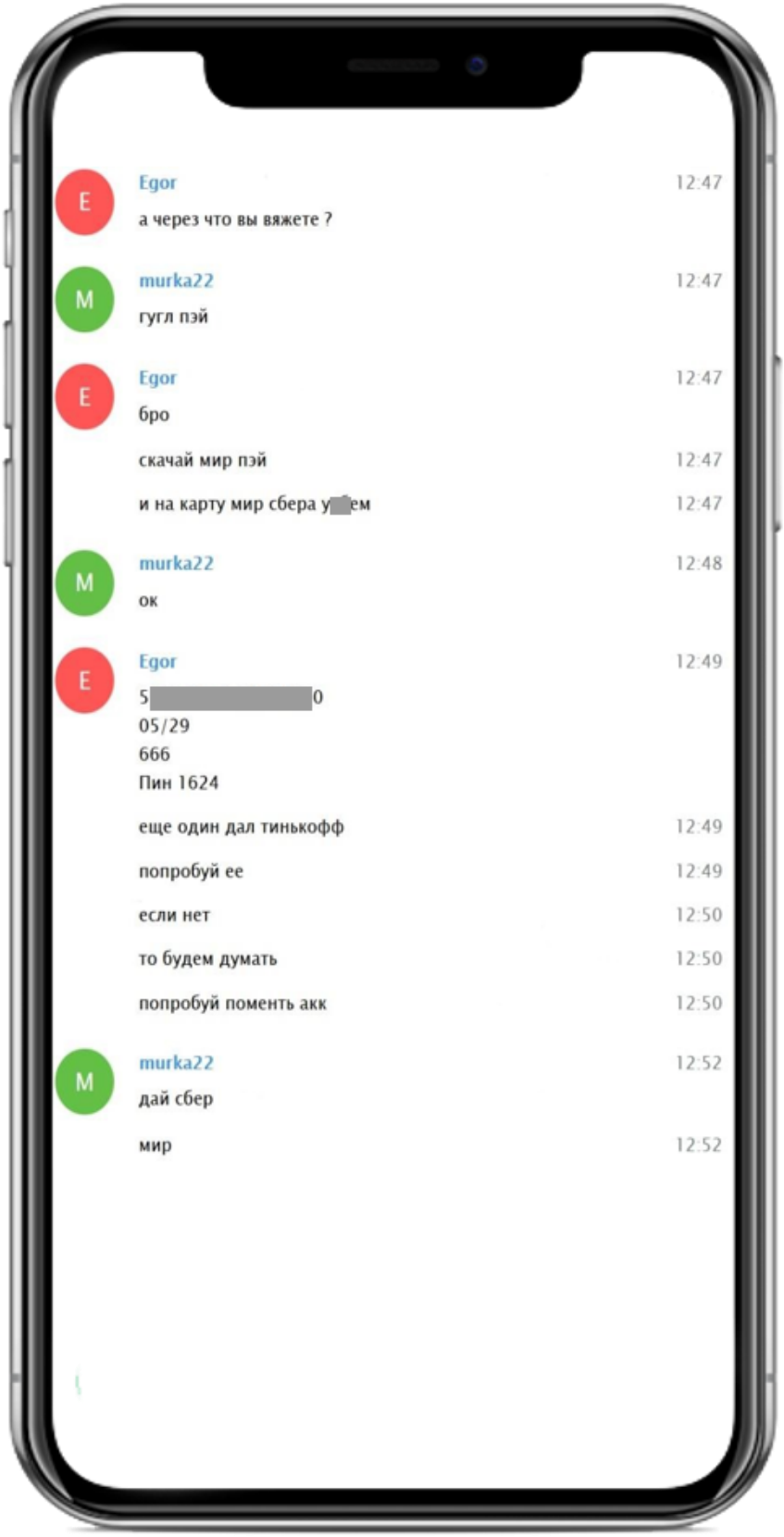


Рисунок 26. Переписка мошенников о привязке дроперской карты

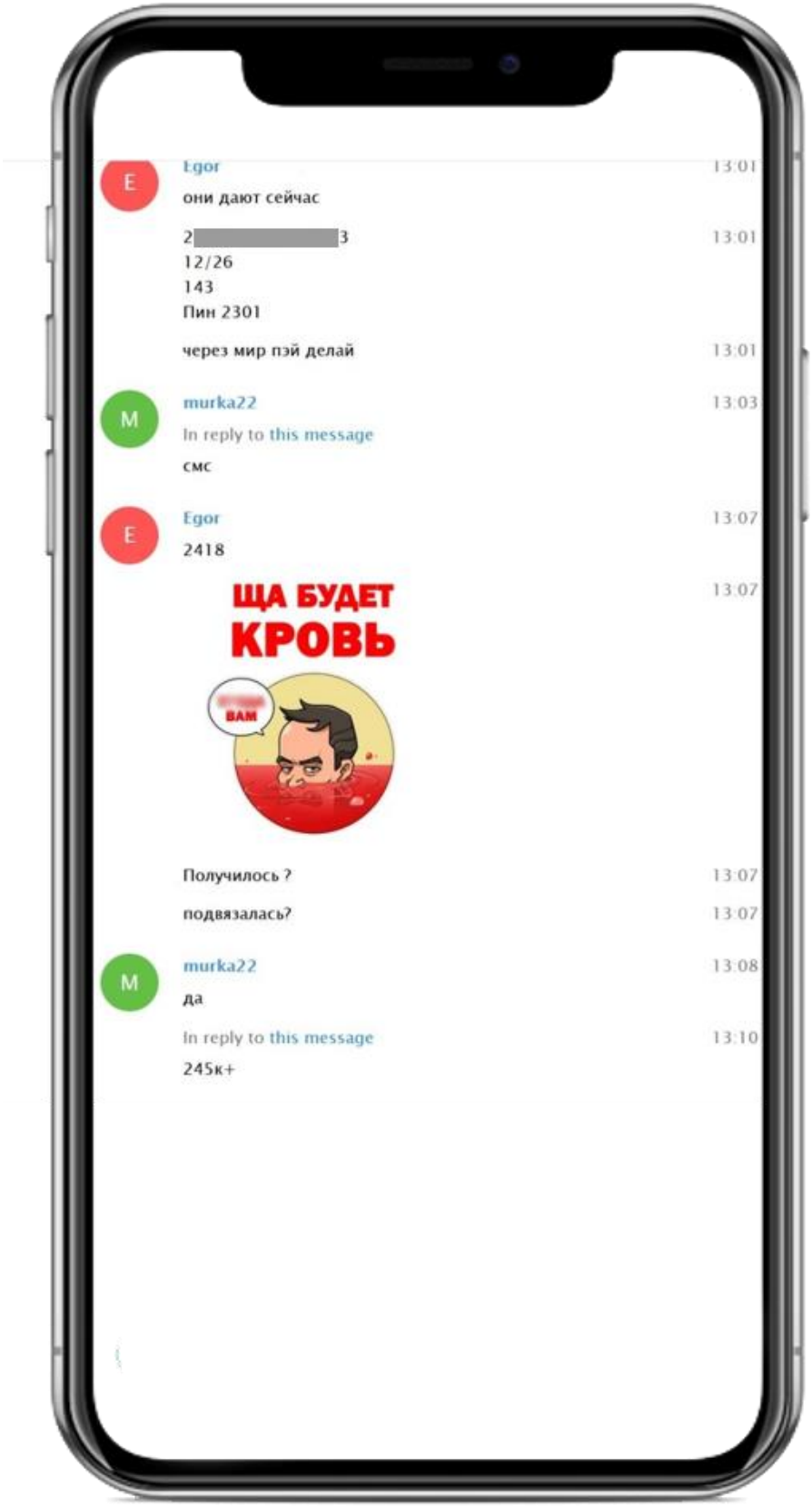


Рисунок 27. Переписка мошенников о привязке дроперской карты

2.4. Вывод похищенных средств

Вывод похищенных денежных средств осуществлялся через специальные сервисы по обналичиванию средств. Данные сервисы широко представлены на специализированных Интернет-площадках и предлагают услуги как по продаже дроперских карт или счетов, так и полной поддержке всего процесса вывода украденных денежных средств со счетов физических и юридических лиц, электронных платежных систем (Яндекс, Qiwi, WebMoney, различных мерчантов, Банков эквайеров, BTC-кошельков и т.д.).

Бердянский call-центр сотрудничал с несколькими сервисами («Tarantino Obnal», «EuroKassa», «Mr.NoBody»). Эти сервисы находятся в теневом Интернет-сегменте, на известных в криминальном мире торговых площадках DarkMoney и Dublikat (рисунок 28 и 29).

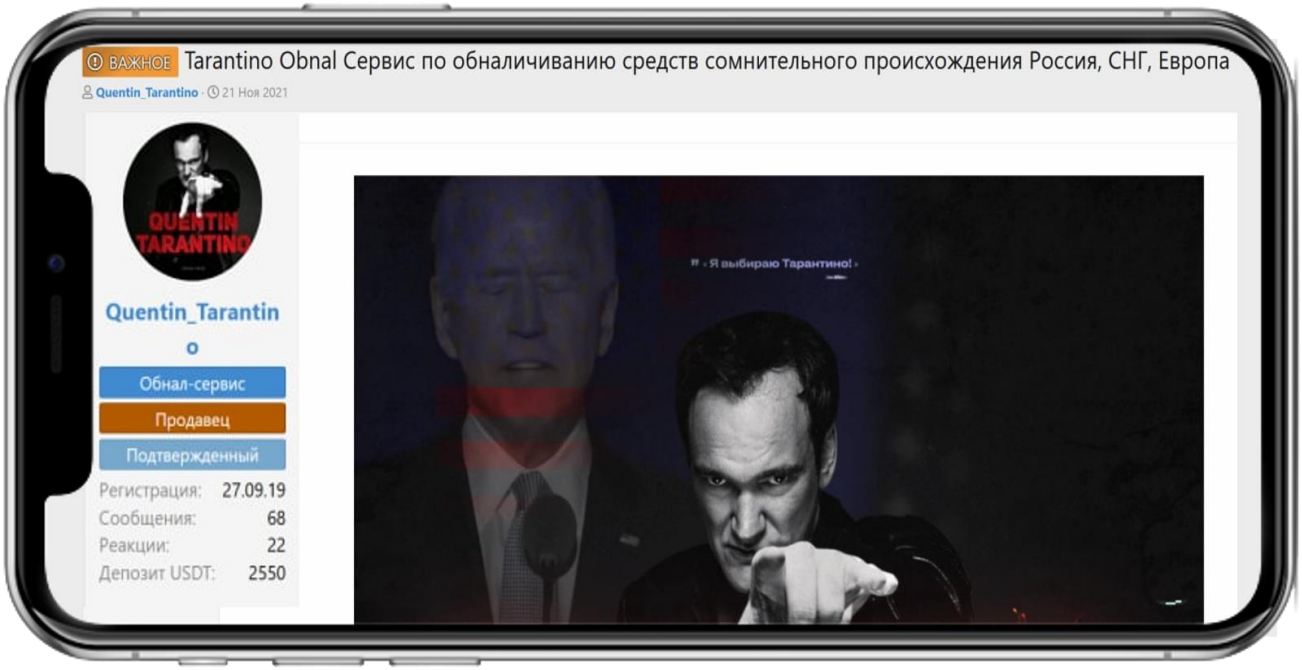


Рисунок 28. Сервис по обналичиванию средств «Tarantino Obnal»

Рисунок 29. Сервис по обналичиванию средств

Процесс вывода денежных средств был организован следующим образом: сотрудники call-центра чаще всего второй линии в режиме разговора с жертвой заказывали через обнал-сервис подходящую карту «дропа» с необходимым лимитом для вывода денег. Персональный менеджер сервиса, закреплённый за данным call-центром в режиме онлайн предоставлял данные и ждал зачисления похищенных у клиента средств. Затем деньги обналичивались сотрудниками сервиса (рисунок 30). Комиссия, в размере от 15 до 20 %, забиралась сервисом, а оставшиеся денежные средства переводились на подконтрольные организаторам call-центра криптокошельки по курсу на текущую дату.

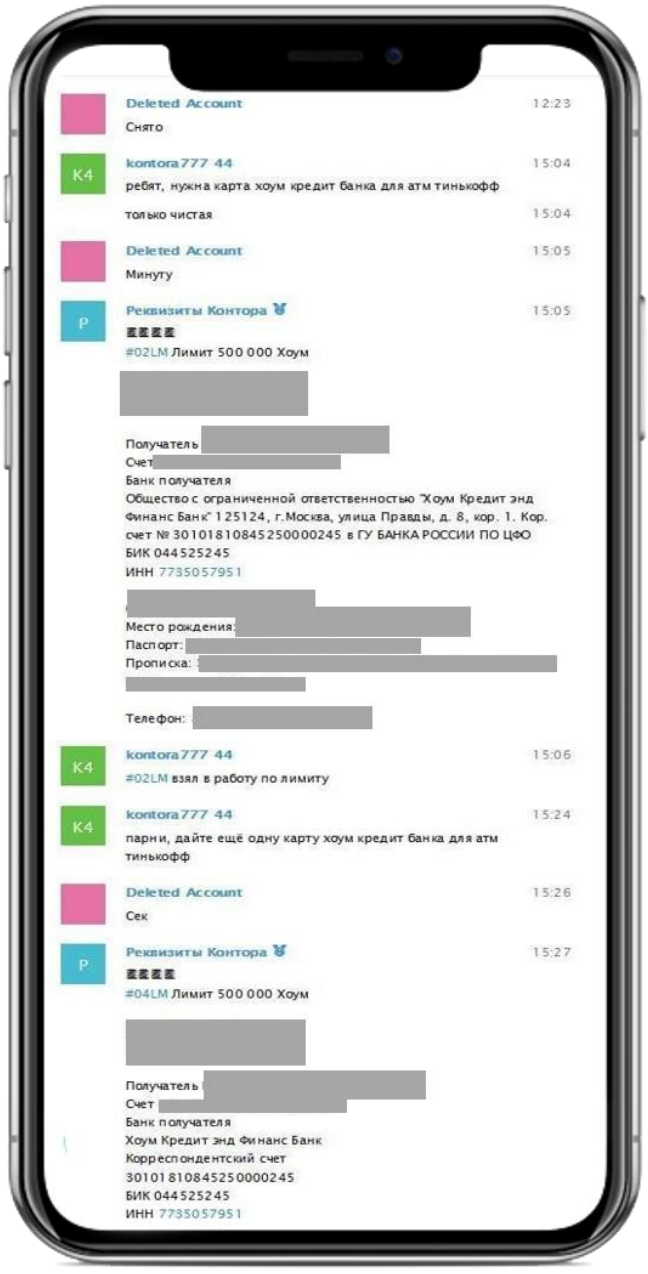


Рисунок 30. Организация вывода средств

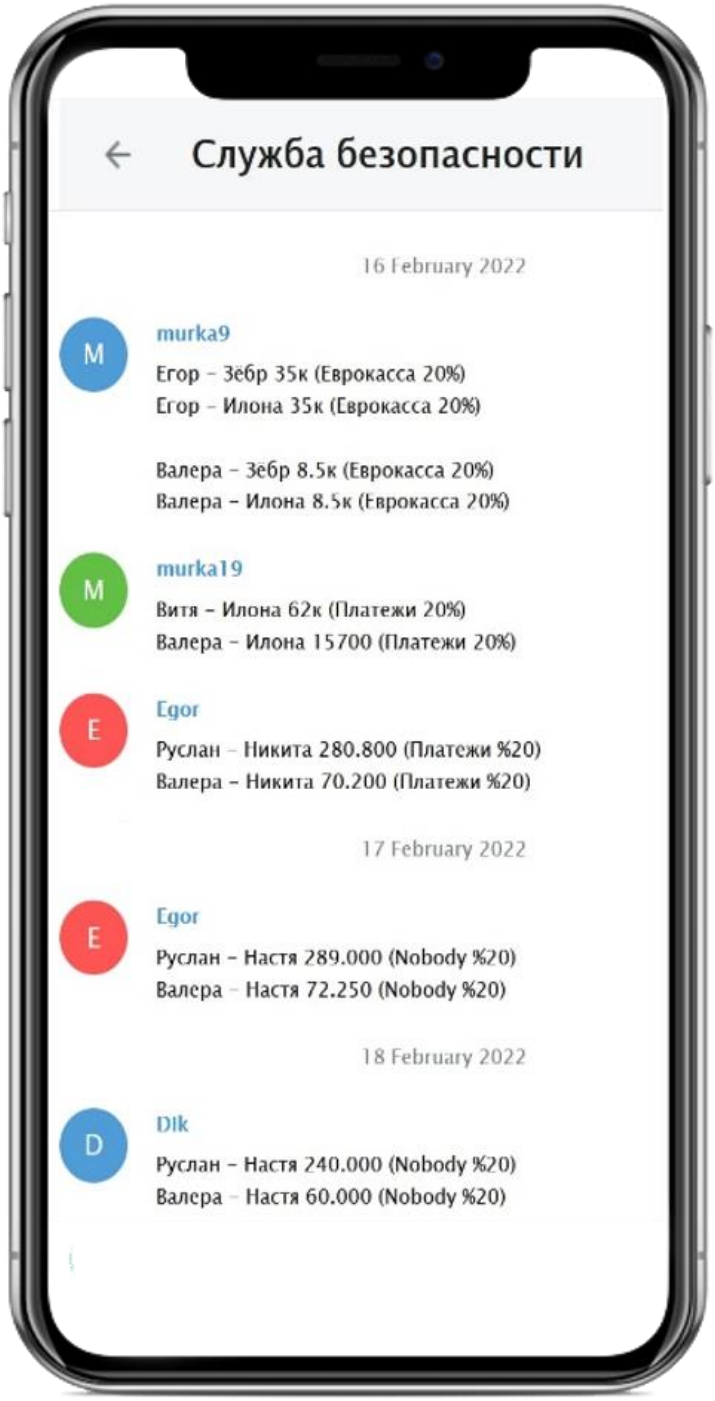


Рисунок 31. Отчеты об украденных суммах

В конце рабочего дня, в рабочих чатах Telegram сотрудники call-центра отчитывались о суммах украденных денежных средств (рисунок 31). Сумма, как правило, включала в себя комиссию сервиса по обналичиванию денежных средств. Также установлено, что такие сервисы дополнительно могут предлагать при оплате повышенной комиссии т.н. «гарантии выплаты» – выплата гарантируется даже в случае, если денежные средства, зачисленные на счет, будут заблокированы службами безопасности банков (рисунки 32,33).

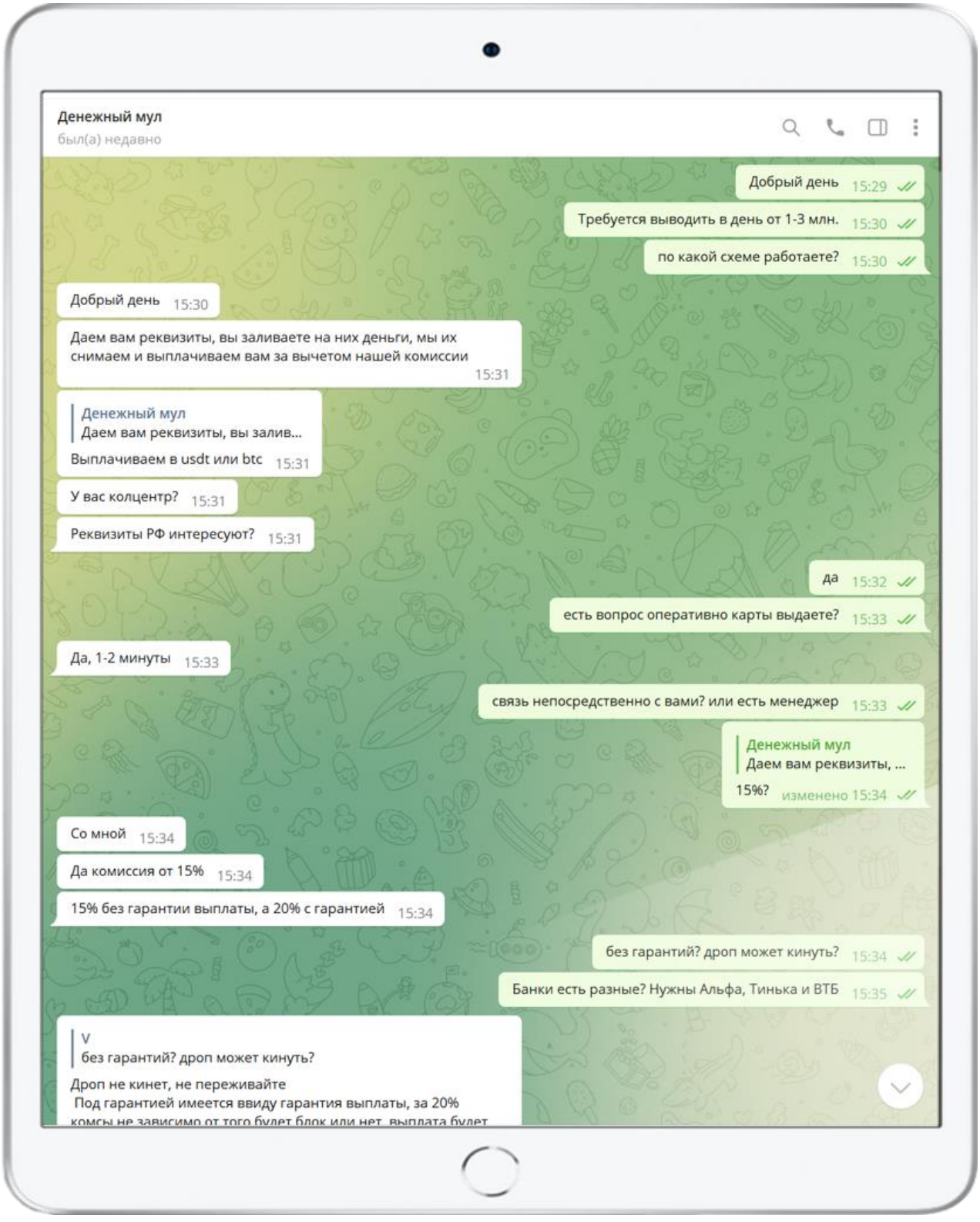


Рисунок 32. Переписка сотрудника мошеннического call-центра с сотрудником сервиса по выводу похищенных средств

Рисунок 33. Переписка сотрудника мошеннического call-центра с сотрудником сервиса по выводу похищенных средств (продолжение Рисунка 32)

В данном call-центре сервис переводил похищенные и обналиченные средства руководителям call-центра через bitcoin-кошельки криптовалютной биржи Binance. В результате анализа рабочей переписки сотрудников call-центра выявлена часть кошельков (см. Приложение 3), используемых для расчетов (35 Bitcoin-криптокошельков).

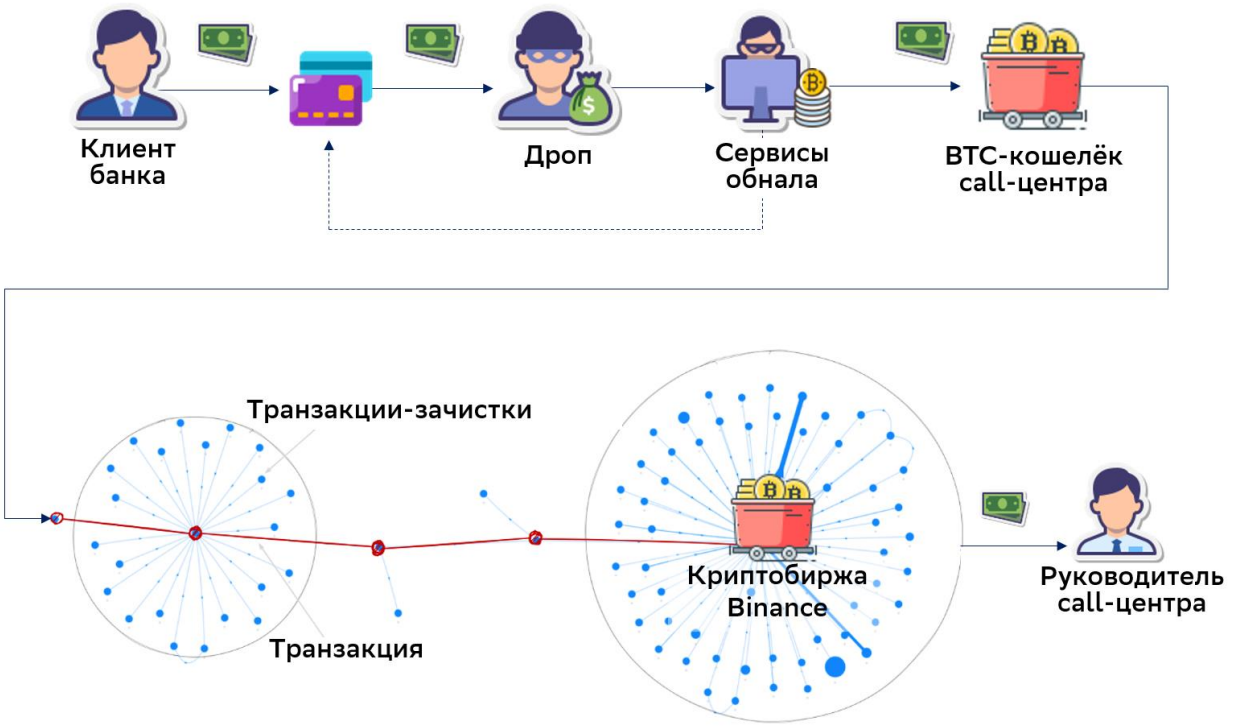


Рисунок 34. Схема обанличивания денежных средств

Общая сумма, проведенная только через указанные криптокошельки составила около 113 тысяч долларов США. Криптокошельки использовались разово, на примере криптокошелька bc1qv3wf936pc55e4ct3g54t400f8auvjhawegdewz видно, что всего было совершено две транзакции: первая транзакция – зачисление денежных средств от «сервиса обнала» в размере 0.02318152 BTC (470,83 $) и вторая транзакция вывода в размере 0.02318152 BTC (470,83 $), (рисунок 35).

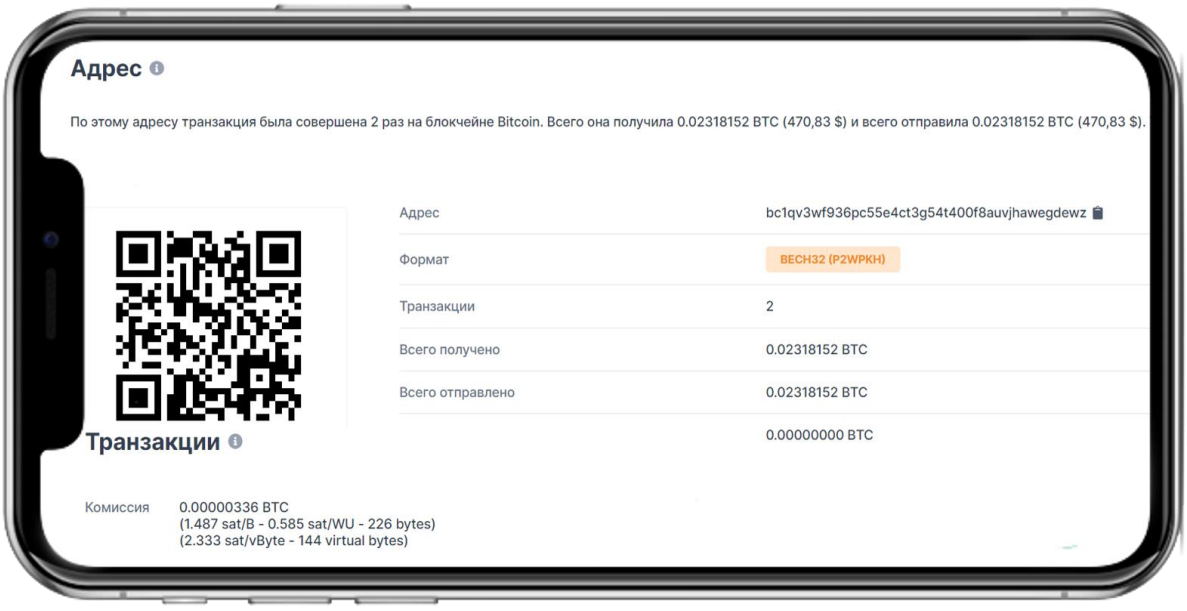


Рисунок 35. Пример транзакций на одном из мошеннических Bitcoin-кошельков

Необходимо отметить, что схема вывода денежных средств позволяла руководству call-центра получать уже «чистые» средства. Обнаружить или отследить украденные денежные средства, выведенные таким способом, практически невозможно.

2.5. Подготовка сотрудников

Все новые сотрудники проходили обучение в обязательном порядке. Типовой процесс обучения хорошо освещен в передаче Андрея Малахова «Прямой эфир», посвященной украинским мошенническим call-центрам[42]. Дополнительно в данном call-центре использовался видеокурс, посвященный обучению работе с конструктором фишинговых сайтов. Необходимо отметить, что конструктор был нацелен на множество российских банков.

Конструктор сайтов дает возможность мошеннику создавать «личный кабинет» под каждого клиента во время разговора. Для этого злоумышленник запрашивает у жертвы максимальный набор данных по ее банковским продуктам (задаются вопросы о счетах и картах, последних совершенных операциях, балансе и так далее). После того, как сбор данных завершен, мошенник создает html-страницу через меню конструктора. Данная страница полностью воссоздаёт личный кабинет жертвы с ее продуктами и остатками. Теперь злоумышленник может демонстрировать клиенту якобы работу с его личным кабинетом, присылая скриншоты поддельного личного кабинета.

На случай, если у жертвы возникают сомнения во время разговора с мошенниками, в конструкторе имеется возможность автоматически создавать поддельные документы и справки от имени банков и правоохранительных органов (рисунки 37, 38).

В конструкторе представлено порядка 40 шаблонов для моделирования сайтов различных банков РФ, например, Сбербанк-Онлайн (рисунок 36). Моделируемые сайты визуально обладают высоким качеством и схожестью с оригинальными сайтами, что позволяет ввести в заблуждение даже опытного пользователя.

[42] https://kino-russfilmi.ru/pryamoj-efir-v-logove-telefonnyh-moshennikov-10-11-2021_055/

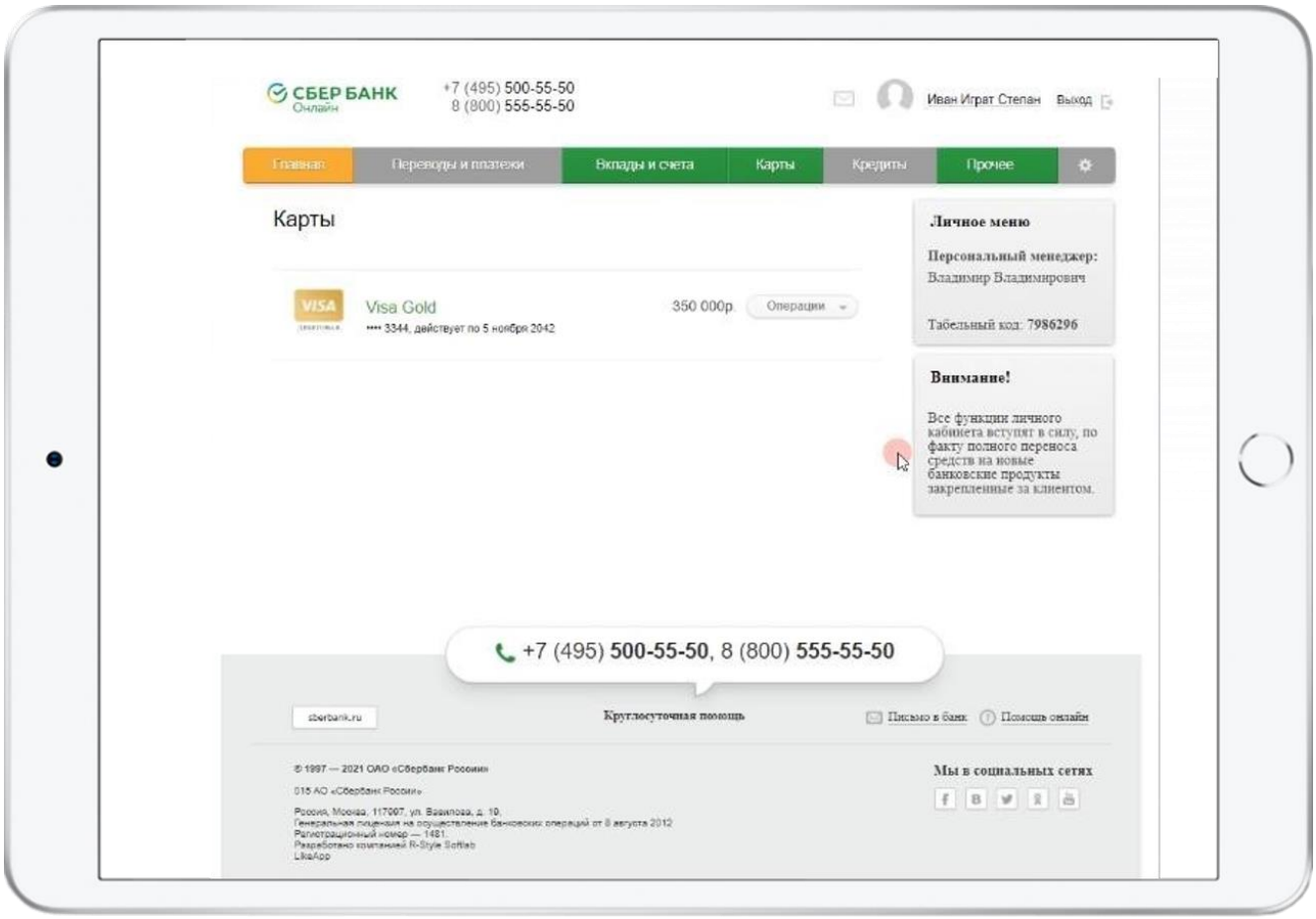


Рисунок 36. Экран Сбербанк-Онлайн, созданный с помощью конструктора фишинговых сайтов

Тинькофф Банк

Исх. № 75121865

По месту требования

Документ № 75121865

Акционерное общество «Тинькофф Банк» сообщает, что остаток сейфовой ячейки г-ки/на Трофимова Ольга Сергеевна по состоянию на 31.01.2022 составляет:

Тип счета	Номер счета	Срок действия:	Код безопастности:	Пин код:
Единый лицевой счет	[redacted]	[redacted]	[redacted]	[redacted]
Страховая ячейка	[redacted]			

Сейфовая ячейка была предоставлена для страхования средств.

Сумма страхования: 1 000 000.00 руб

Страховой партнер: Тинькофф Банк
Специалист кредитного отдела: [redacted]
Ответственное лицо за ячейку:

Реквизиты банка: [redacted]
Банк: Головной офис АО «Тинькофф Банк»
БИК: 044525974
ИНН: 7710140679
Корр.сч.: 30101810014525000974
Расчетный счет(лицевой): 30232810100000000004

Зам. Начальника ОПИО РОО "Москва" Тинькофф (АО)
М.П.

Акционерное общество «Тинькофф Банк» Управление обработки заявлений Для документов г. Москва

А.М. Колесников

Тинькофф Банк

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 2LCG69A17NRGSZQU4V3XIO8FBHTPM0D5YW
Владелец **А.М. Колесников**
Действителен с 14.06.2021 по 9.09.2022

АО «Тинькофф Банк» | Головной офис АО «Тинькофф Банк» | 1-й Волоколамский проезд, д.10, стр.1 г.Москва 123060 | Телефон: (495) 64-81-000 Факс: (495) 645-59-09 | S.W.I.F.T.: TICSRUMMXXX E-mail: cso@tinkoff.ru

Рисунок 37. Поддельный банковский документ

Исх. № 18108758

По месту требования

Документ № 18108758

Банк ПАО «Сбербанк» настоящим письмом уведомляет, что Вы, [redacted], стали жертвой мошеннических действий. Для обеспечения безопасности финансовых активов, согласно договора банковского обслуживания, необходимо выполнить процедуру обновления единого номера лицевого счета.

Специалист финансового отдела: [redacted]
Финансово-ответственное лицо*: ожидает активации

** Обращаем Ваше внимание, получатель является финансово-ответственным лицом.*
** Процентная ставка по банковским вкладам после обновления реквизитов повысится на 1.5% годовых.*
** После обновления реквизитов все финансовые активы, которые находились на счетах клиента до мошеннических действий будут восстановлены.*

Банк приносит свои извинения за сложившуюся ситуацию. Мы сделаем все для того, чтобы в дальнейшем Вы не оказались в подобной ситуации.

Реквизиты банка:
Банк: Филиал №1587 Сбербанка (ПАО) г.Москва
БИК: 044525225
ИНН: 7707083893
Корр.сч.: 30101810400000000225

Зам. Начальника ОПИО РОО
"Москва" филиала №1587
СберБанка (ПАО)
М.П.

А.М. Колесников

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат S0G3GB2XK8579PVCFRTQIND6AEYLMH4U1O
Владелец **А.М. Колесников**
Действителен с 12.06.2021 по 21.09.2022

Банк Сбербанк (публичное акционерное общество) | ОО "Москва" Филиал №1587 Сбербанк (ПАО) | ул. Вавилова, 19 г.Москва 117997 | Телефон: (4722) 30-50-00, 54-33-06 Факс: (4722) 30-50-00 | S.W.I.F.T.: SBERRUMM E-mail: info@sb.ru

Рисунок 38. Поддельный банковский документ

3. ТЕХНОЛОГИИ В РАБОТЕ CALL-ЦЕНТРА «БЕРДЯНСК»

3.1. Программное обеспечение на рабочих местах

Как было сказано выше, всего в офисе call-центра находилось порядка 70 рабочих мест. На рабочих станциях сотрудников call-центра была установлена не лицензированная (пиратская) версия операционной системы (далее – ОС) Windows 7 с использованием общедоступных в сети Интернет лицензионных ключей. Активация ОС не проводилась.

Рабочие станции call-центра не были привязаны к домену и находились в рабочей группе сети WORKGROUP, доменная инфраструктура отсутствовала. Сотрудники работали под учетной записью локального администратора. Для подключения офиса к сети Интернет использовался Интернет-провайдер «Onet» (http://onet.zp.ua/, г.Бердянск, ул. Красная, 4А). Типовой набор используемого ПО включал в себя следующее:

- Veracrypt – полное шифрование данных на жестком диске;
- PhonerLite, Microsip, X-Lite, Zoiper5 – клиентская часть ПО для ip-телефонии, используемая для обзвона;
- Malwarebytes – антивирус;
- TelegramDesktop, Slack – чаты для общения сотрудников между собой постановки задач и передачи рабочих материалов;
- Whatsapp, Viber – чаты для общения сотрудников с жертвами;
- Proxyfier – proxy-клиент.
- CRM-система собственной разработки под наименованием «CRM BRO»

Все используемое ПО является бесплатным или условно бесплатным. Также на рабочем месте одного из организаторов call-центра обнаружены скрипты для автоматизации сбора персональных данных владельцев номеров телефонов: Python-скрипты для мессенджера Telegram, позволяющие оперативно запрашивать и пересылать информацию из специализированных Telegram-ботов пробива данных в рабочие Telegram группы.

3.2. Инструменты телефонии и «сопровождения» клиентов

Мошенниками активно использовалась облачная инфраструктура, в частности, серверы SIP-телефонии располагались в Германии, Франции, США, Великобритании и Эстонии. Для обзвона использовались серверы в различных странах Европы. Вот некоторые из них:

- 95.217.157.115 (Германия);
- joicephone.com (Германия);
- sip.freevoip.org (США);
- 194.28.164.19 (Великобритания);
- sip.nonamevoip.com (Cloudflare, США);
- 212.83.140.211 (Франция);
- rdx.narayana.im (Эстония);
- 212.83.175.208 (Франция).

На изображениях ниже представлен пример личного кабинета на ресурсе «rdx.narayana.im». Данный сервис является наиболее известным VOIP-ресурсом для осуществления мошеннических звонков украинских call-центров гражданам РФ.

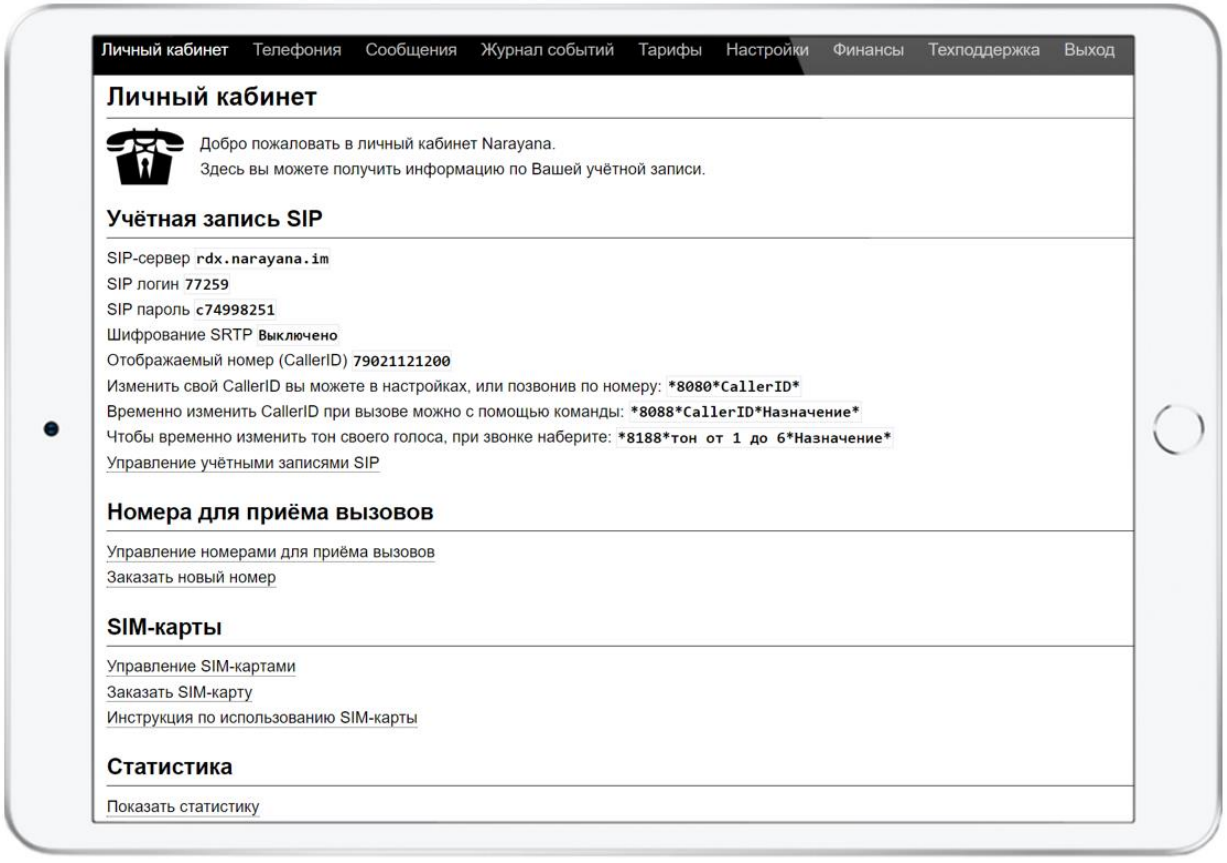
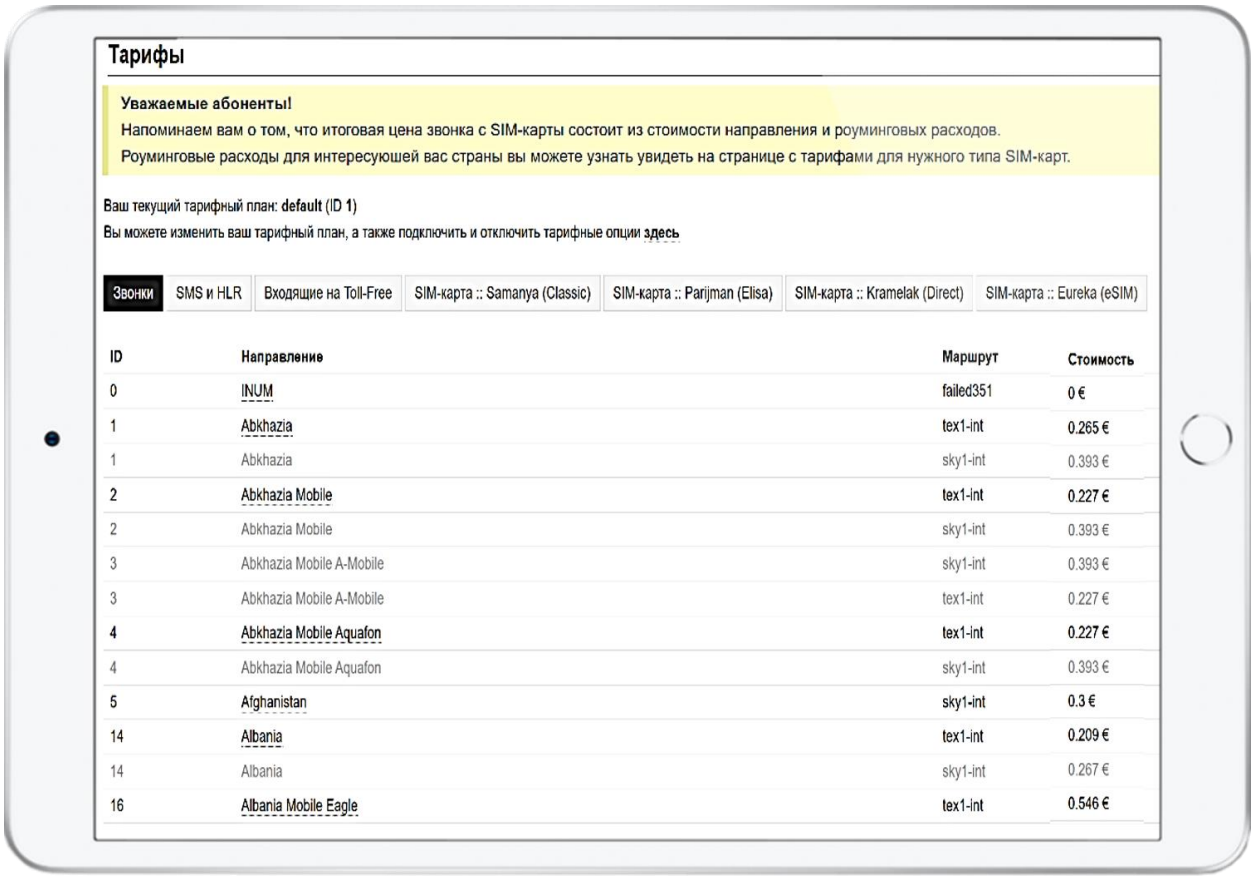


Рисунок 39. Параметры учетной записи одного из SIP-сервисов



Тарифы

Уважаемые абоненты!

Напоминаем вам о том, что итоговая цена звонка с SIM-карты состоит из стоимости направления и роуминговых расходов.

Роуминговые расходы для интересуюшей вас страны вы можете узнать увидеть на странице с тарифами для нужного типа SIM-карт.

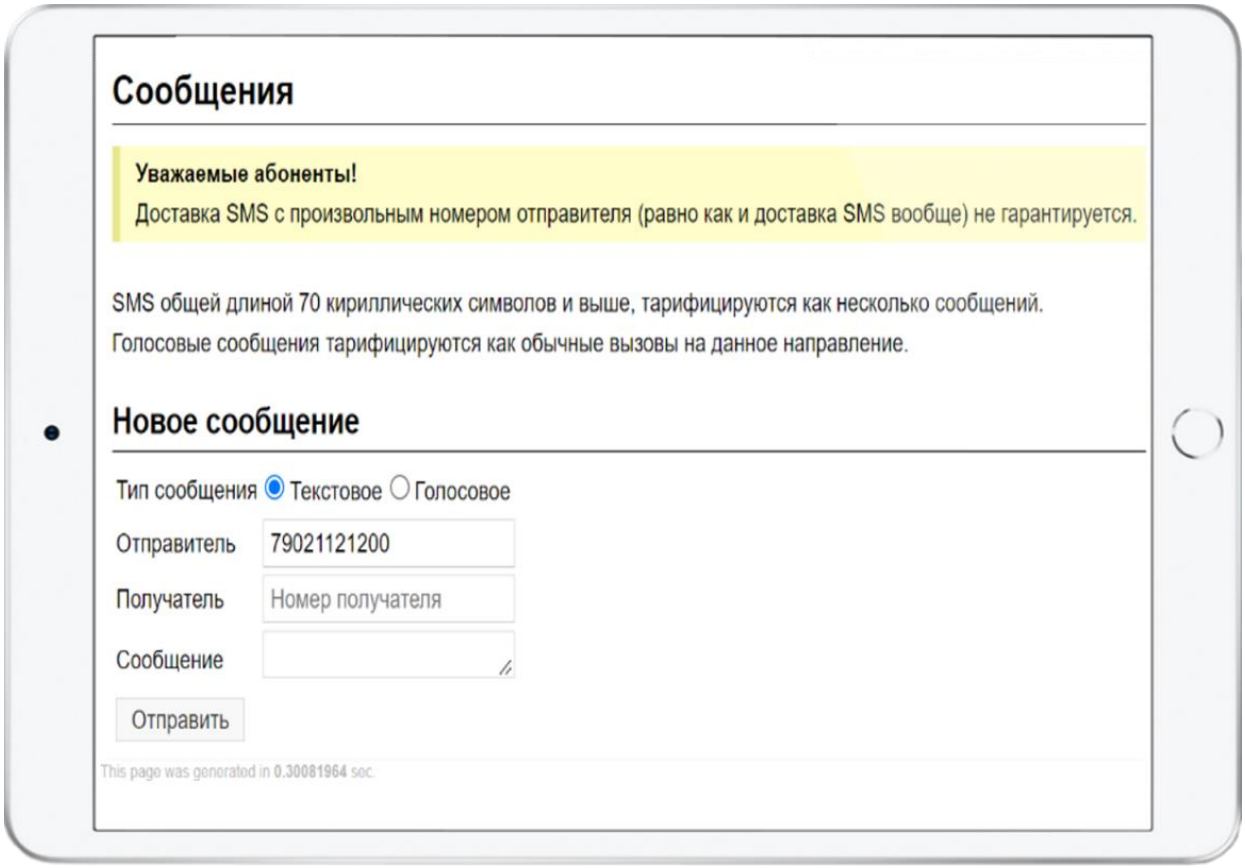
Ваш текущий тарифный план: **default** (ID 1)

Вы можете изменить ваш тарифный план, а также подключить и отключить тарифные опции здесь

Звонки | SMS и HLR | Входящие на Toll-Free | SIM-карта :: Samanya (Classic) | SIM-карта :: Parijman (Elisa) | SIM-карта :: Kramelak (Direct) | SIM-карта :: Eureka (eSIM)

ID	Направление	Маршрут	Стоимость
0	INUM	failed351	0 €
1	Abkhazia	tex1-int	0.265 €
1	Abkhazia	sky1-int	0.393 €
2	Abkhazia Mobile	tex1-int	0.227 €
2	Abkhazia Mobile	sky1-int	0.393 €
3	Abkhazia Mobile A-Mobile	sky1-int	0.393 €
3	Abkhazia Mobile A-Mobile	tex1-int	0.227 €
4	Abkhazia Mobile Aquafon	tex1-int	0.227 €
4	Abkhazia Mobile Aquafon	sky1-int	0.393 €
5	Afghanistan	sky1-int	0.3 €
14	Albania	tex1-int	0.209 €
14	Albania	sky1-int	0.267 €
16	Albania Mobile Eagle	tex1-int	0.546 €

Рисунок 40. Тарифы на SIP-телефонию



Сообщения

Уважаемые абоненты!

Доставка SMS с произвольным номером отправителя (равно как и доставка SMS вообще) не гарантируется.

SMS общей длиной 70 кириллических символов и выше, тарифицируются как несколько сообщений.

Голосовые сообщения тарифицируются как обычные вызовы на данное направление.

Новое сообщение

Тип сообщения (•) Текстовое ( ) Голосовое

Отправитель 79021121200

Получатель Номер получателя

Сообщение

Отправить

This page was generated in 0.30081964 sec.

Рисунок 41. Отправка SMS-сообщений с помощью SIP-телефонии

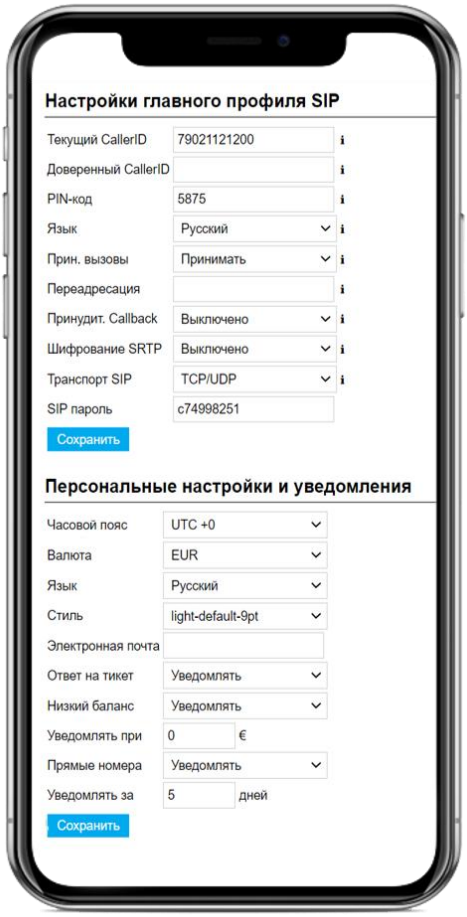


Рисунок 42. Настройки SIP-телефонии

В ходе исследования обнаружены учетные данные для входа на серверы SIP-телефонии, что позволило установить всю цепочку осуществления мошеннических звонков гражданам РФ. Вся обнаруженная информация передана сотрудникам полиции для приобщения к материалам уголовных дел.

Для сервиса Narayana регистрация нового пользователя бесплатна, минимальный первый платеж составляет 51 евро или эквивалент в другой валюте. При регистрации не требуется указывать личные данные, в т.ч. адрес электронной почты. Предоставляемые услуги доступны при использовании VPN, Proxy-серверов, также сайт доступен в сети «TOR».

Цены на звонки по России составляют от 0.065 до 0.39 евро за минуту/SMS сообщение/1 мб данных. Стоимость одного виртуального номера зависит от страны и начинается от 10 евро в месяц, можно заказать SIM карту за 20 евро.

Для организации работы сотрудников call-центра использовалась CRM-система (рисунок 43), размещенная в Интернет-облаке и закрытая средствами защиты и контроля доступа американской компании Cloudflare (https://taep38xor5m.xyz/wen2uab/). Установлено, что в данной CRM

хранилась и обрабатывалась база «клиентов» и формировались поддельные финансовые справки и документы для них.

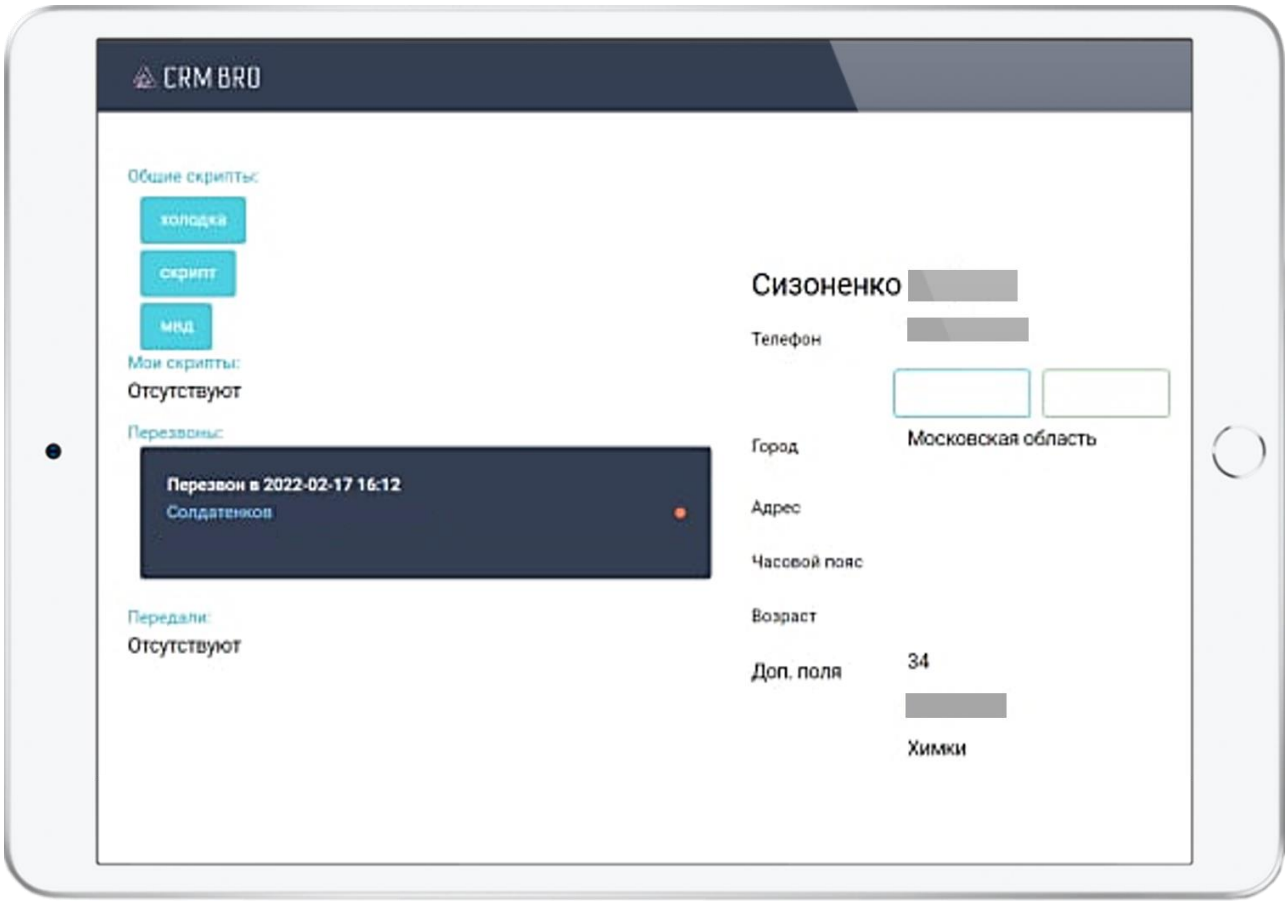


Рисунок 43. CRM-система, которую использовали мошенники в бердянском call-центре (персональные данные жертвы скрыты)

CRM-система, используемая сотрудниками КЦ позволяла операторам оперативно вносить информацию о клиентах (будущих жертвах). При обзвоне по базам данных, оператором первой линии в CRM заполнялись поля ФИО, телефон, адрес места жительства, возраст клиента и другая доп. информация. В случае если клиенту не удавалось дозвонится до клиента ставила метка «недозвон» и клиенту мог звонить уже другой оператор первой линии. При успешном перезвоне, помечалась дата звонка и фамилия звонившего.

Также для оперативной проверки данных банковской карты в нижней части системы было расположено окно проверки банковских карт, в которой сотрудник КЦ мог проверить достоверность данных, полученных от клиента (определить по BIN-у и номеру какому банку принадлежит карта). Если в ходе общения с клиентом оператором была получена вся необходимая информация, то он передавался операторам второй линии. Если же в ходе общения с клиентом была получена информация, что у него нет остатков по денежным счетам, ему присваивалась метка «нет средств» и в дальнейшем ему

перезванивали спустя какое-то время. Если во время разговора жертва понимала, что ему позвонили мошенники, то они оставляли пометку «умник» в его профиле CRM. Также дополнительно помечали кому можно перезвонить или до кого не получилось дозвониться. В случае успешного мошеннического списания клиенту добавляли пометку «списали».

3.3. Системы коммуникаций и анонимизации

Для работы сотрудников call-центра использовались Proxy-серверы только российских провайдеров, чтобы обходить возможные блокировки и скрыть факты работы из Украины. Установлено использование 19 proxy-серверов российских Интернет-провайдеров P***** IT Ltd, A***** LLC, C***** Ltd, Q***** LLC (полные наименования раскрывать не можем в интересах следствия). При этом 16 из них расположено в Москве, остальные – в Казани, Саратове и Санкт-Петербурге. Информация о серверах передана в правоохранительные органы.

Для коммуникаций внутри call-центра использовали мессенджер Slack, однако с середины 2021 года злоумышленники постепенно перевели все свои коммуникации в Telegram. Для регистрации Telegram-аккаунтов использовались виртуальные номера телефонов. Такие номера можно свободно приобрести на специализированных Интернет-площадках. Детали по данным номерам и площадкам переданы в правоохранительные органы.

Одной из особенностей организации защиты call-центра является усиленные процедуры защиты информации на рабочих станциях. Так, жесткие диски на всех рабочих местах были зашифрованы с помощью ПО Veracrypt, а длина пароля на некоторых компьютерах составляла более 40 символов.

Также для работы использовались подключаемые криптоконтейнеры с объемом хранимых данных более 50 Гб. Информация с данных криптоконтейнеров после расшифрования стала основой для написания данного отчета и дальнейшей работы с полицией. В результате расшифрования данных контейнеров получена значимая информация о работе данного call-центра: базы данных с информацией по клиентам, в т.ч. списки пострадавших, базы для обзвона, аудиозаписи разговоров с клиентами, скрипты разговоров и персональная информация сотрудников call-центра.

Сотрудники call-центра использовали сложные пароли, которые генерировались с помощью специализированных программных средств автоматически или вручную, с соблюдением необходимых требований к надежности и защите от перебора.

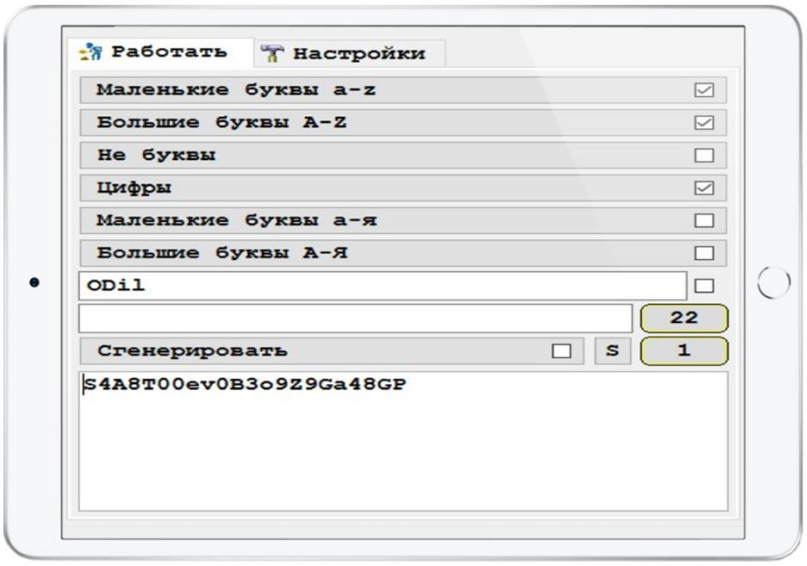


Рисунок 44. ПО для генерации паролей, используемых в call-центре

Пароли от криптоконтейнеров содержали случайные комбинации букв верхнего и нижнего регистра латинского, русского алфавитов, цифры, спецсимволы и достигали длины до 40 символов.

3.4. Идентификация сотрудников call-центра

В середине апреля 2022г. по факту ликвидации call-центра сотрудниками ФСВНГ Росгвардии на российских ТВ-каналах вышли новостные сюжеты[43] с кадрами из пустующих помещений. При этом часть информации и личных вещей, брошенных сотрудниками, на рабочих местах осталось и попало в кадры видеосюжетов.

В ходе изучения фотографий и видеорепортажей были обнаружены в том числе плакаты с именами и датами рождения сотрудников call-центра (рисунок 45). Анализ данной информации, а также информации, собранной с компьютерной техники call-центра, несмотря на применяемых меры безопасности, позволил установить значительное число его предполагаемых сотрудников – граждан Украины.

[43] https://tvzvezda.ru/news/2022415259-KxrTx.html

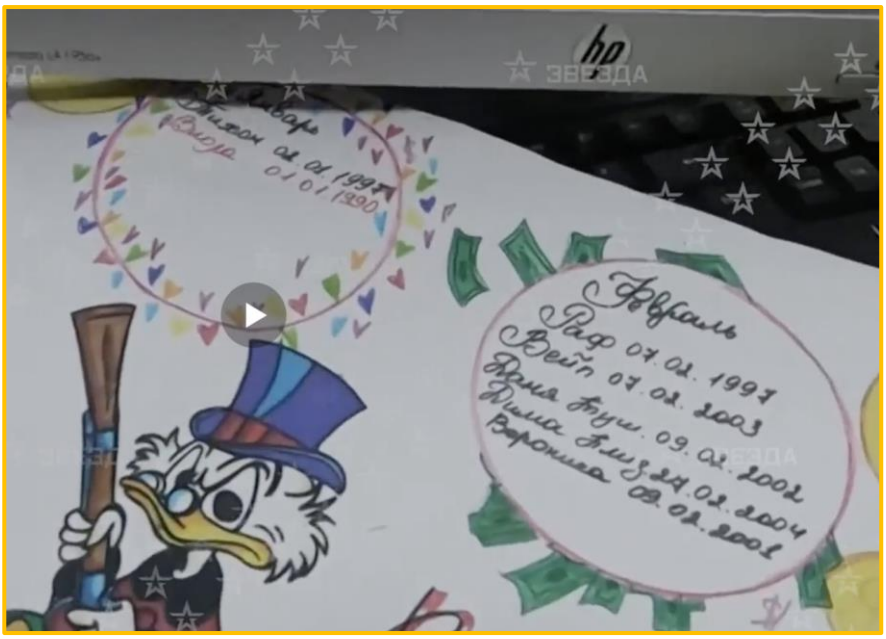


Рисунок 45. Кадры с репортажем о деятельности call-центра с информацией о датах рождения сотрудников

Вся информация передана сотрудникам правоохранительных органов. В данном отчете с разрешения российских правоохранительных органов мы приведем только некоторых из установленных сотрудников.

Одним из основных участников call-центра является Шестаков Данил Андреевич, который в настоящее время находится на территории РФ. Данный сотрудник нарушил главное правило call-центра – сотрудникам запрещено заходить в социальные сети с рабочих ПК, а также размещать фотографии с рабочего места и на одном из компьютеров удалось найти сессию авторизации в социальной сети Вконтакте личной страницы Шестакова Д. (Рисунки 46, 47).

ype	Link	Last visit ti...
	https://vk.com/login.php?u=2&to=/login.php	22.02.2022 14:47:50
	https://vk.com/login.php?act=slogin&role=fa	22.02.2022 14:47:50
	https://login.vk.com/?role=fast&_origin=http	22.02.2022 14:47:50
	https://vk.com/login.php?op=logout&hash=	22.02.2022 14:47:50
	https://login.vk.com/?act=logout&hash=02c	22.02.2022 14:47:50
	https://vk.com/	22.02.2022 14:47:50

Рисунок 46. Адрес личной страницы Шестакова Д.А. в социальной сети Вконтакте

Рисунок 47. Фотография с личной страницы Шестакова Д.А.

Изучив данную страницу, удалось установить, что Шестаков Данил Андреевич 13.08.2000 г.р. проживал в г. Бердянск, в настоящее время проживает в г. Судогда, Владимирской обл. Также в ходе анализа социальных сетей была найдена его вторая страница в ВК, где Шестаков Д.А. указал, что он проживает в г. Бердянск.

Используя открытые источники информации, удалось установить еще одного активного участника – Денисову Дарью 11.02.2002 г.р., являющуюся пользователем социальной Вконтакте (см. рисунок 48).

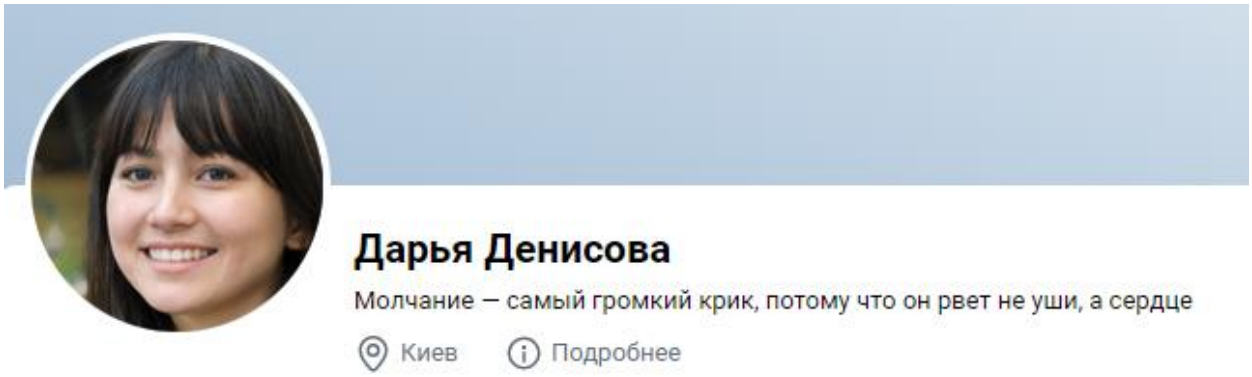


Рисунок 48. Страница Денисовой Д. в социальной сети Вконтакте

Другого сотрудника удалось установить по его редкому имени – Марк Зотов, 05.03.1998 г.р. (рисунок 49). Марк скрывает свои фотографии в социальной сети Вконтакте, однако удалось найти его фото в социальной сети Одноклассники (рисунок 50).

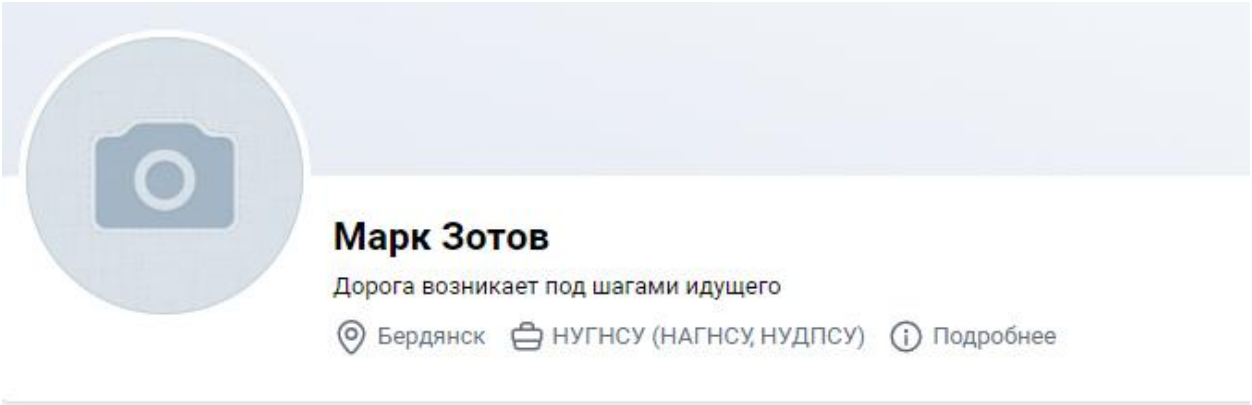


Рисунок 49. Страница Зотова М. в социальной сети Вконтакте

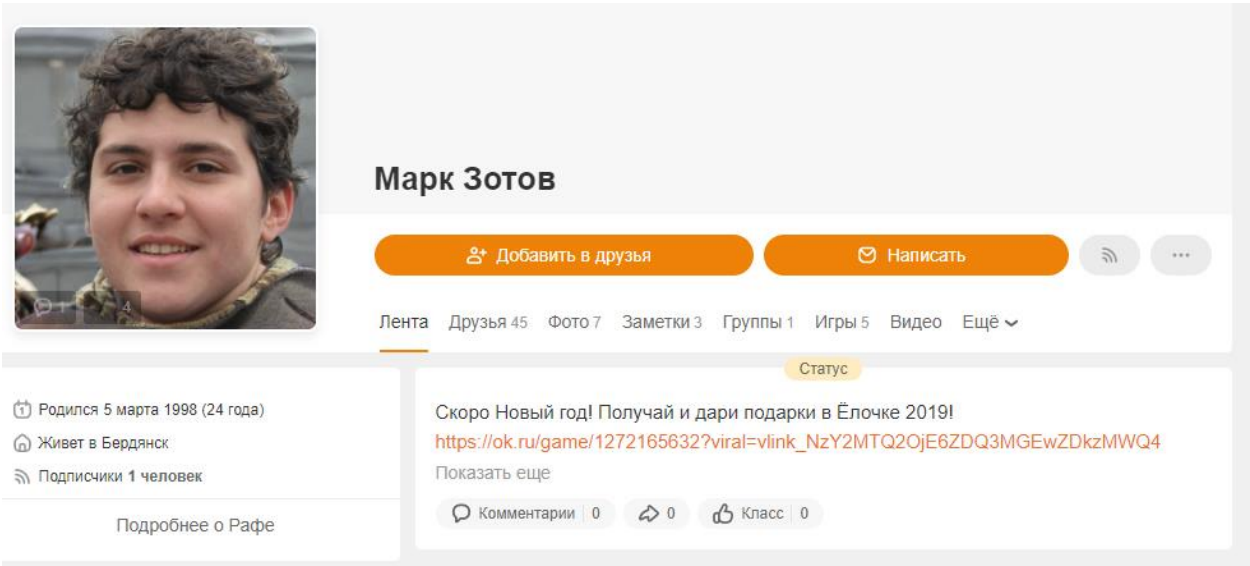


Рисунок 50. Страница Зотова М. в социальной сети Одноклассники

Одним из наиболее ярких сотрудников данного call-центра является также и Нестерова Полина 05.07.1994 г.р. (рисунок 51). Примечательно, что на странице данного сотрудника размещены фотографии с ювелирными украшениями дорогих брендов, по которым сразу становится понятно, куда были потрачены похищенные у граждан РФ денежные средства (рисунок 52).

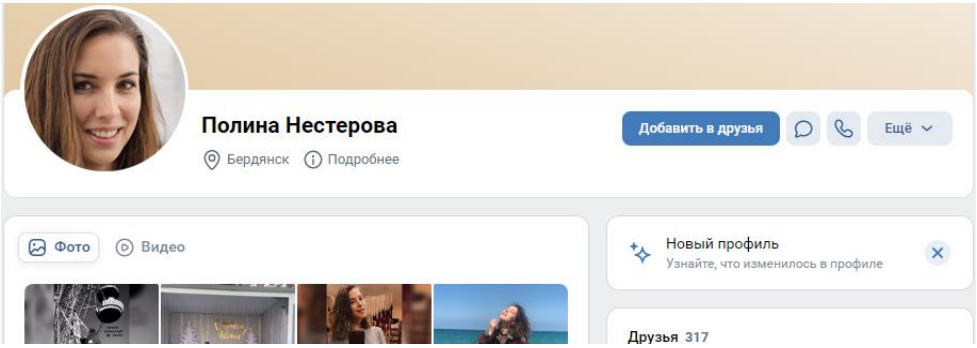


Рисунок 51. Страница Нестеровой П. в социальной сети Вконтакте

Рисунок 52. Фотография со страницы Нестеровой П. в социальной сети Вконтакте

Все сотрудники call-центра, перечисленные в данном разделе, составляют только часть идентифицированных лиц, а собранная в ходе исследования информация (как о технологиях, так и о людях) передана в правоохранительные органы.

В настоящее время Сбер, во взаимодействии с с правоохранительными органами, установил пострадавших клиентов банков от действий бердянского call-центра[44]. В данный момент заведено сотни уголовных дел. Личности сотрудников call-центра установлены и уже известно, что в результате их действий российские граждане понесли многомиллионный ущерб. Доказательная база, в том числе цифровые следы злоумышленников,

[44] Путем сопоставления данных жертв мошенников.

обнаруженные Сбером, изучаются сотрудниками правоохранительных структур, и в ближайшее время все, кто имел отношение к данному call-центру, будут объявлены в розыск. Следующий шаг – довести все дела до суда, чтобы преступники получили соразмерное наказание.

ЗАКЛЮЧЕНИЕ

Основная цель украинских преступных группировок – помимо незаконного обогащения – лежит в области государственной политики Украины, направленной против Российской Федерации [45] . Целенаправленные действия преступников наносят ущерб не только по гражданам РФ, которые лишаются своих накоплений, но и по экономике страны, а также дискредитируют действия российской правоохранительной системы, поскольку мошенники находятся вне досягаемости для российских структур. Задержание преступников, находящихся заграницей, в условиях острой внешнеполитической ситуации, оказывается фактически неосуществимым, даже несмотря на наличие доказательственной базы. Масштаб организации call-центров, описанный в нашем исследовании, позволяет оценить всю глубину этой проблемы на примере одного call-центра, находившегося до начала специальной военной операции в г. Бердянск Запорожской области.

По нашей оценке, несмотря на проводимую специальную военную операцию на территории Украины, количество атак на клиентов банков вышло на уровень до СВО и по нашим оценкам будет только увеличиваться. В первую очередь, это связано с высоким уровнем вовлеченности в преступную деятельность десятков тысяч людей на территории Украины: сотрудников call-центров, организованных преступных сообществ, курирующих их представителей силовых структур, дропов и других. Во-вторых, на фоне тотальной бедности украинского населения и нарастающего русофобского настроения, ожидается рост числа желающих побороться за миллиарды похищенных денежных средств у граждан РФ. Усугубляет ситуацию и фактическое сращивание государства и преступных сообществ, организующих деятельность подобных call-центров.

Мошенническая деятельность организована по образу корпоративной бизнес-индустрии. Данный сегмент криминального мира имеет структурно

[45] https://rtvi.com/news/v-sberbanke-zayavili-chto-ukrainskie-koll-czentry-mogut-vorovat-u-rossiyan-do-130-mln-rublej-v-mesyacz/

разветвленную сеть с «бизнес-процессами», налаженными по аналогии с легальным бизнесом: аренда помещений, зарплаты и бонусы, специальное оборудование и программное обеспечение, конкуренция и запуск новых call-центров по принципу франшизы (таких, как бердянский call-центр). Определенная часть заработка, как и в легальном бизнесе, уходит владельцам (и «покровителям»), а после начала СВО мошенники уже перестали скрывать, что часть средств идет на содержание националистических батальонов ВСУ.

На территории Российской Федерации создание подобных call-центров невозможно поскольку у силовых структур наработана практика их оперативного выявления, ликвидации и привлечения организаторов и участников к уголовной ответственности

По оценкам Сбера без системного решения проблемы телефонного мошенничества наиболее вероятными сценариями дальнейшего развития событий будут являться:

- Кратное увеличение количества call-центров на территории Украины (преимущественно в западной ее части) в ближайшие 2 года. Это будет обуславливаться тяжелой экономической ситуацией, при которой варианты получения достойного заработка будут существенно ограничены.
- Расширение используемых мошеннических схем (атаки на юридические лица, подстрекательство к терроризму[46], в т.ч. поджогам и проч.) и, как следствие, рост количества жертв. Call-центры не остановятся лишь на телефонном мошенничестве: в составе организованных преступных сообществ есть команды, которые специализируются как на фишинге, мошенничестве на маркетплейсах и сервисах объявлений, так и на угрозах семьям российских военнослужащих.
- Миграция организованных преступных сообществ, специализирующихся на таком виде мошенничества, а также атаки на граждан других стран. Все чаще владельцы call-центров ищут сотрудников - нативных носителей языков европейских стран.
- Образование мощных международных преступных синдикатов на основе существующих сообществ, которые будут не только содержать call-центры, но и значительно расширят сферу своей деятельности – от телефонного мошенничества до торговли наркотиками и оружием.

[46] https://iz.ru/1320816/2022-04-14/mvd-zaiavilo-o-sozdanii-vsu-call-tcentrov-dlia-telefonnogo-terrorizma-v-rossii

Для успешного решения текущих проблем необходимо создать препятствия для использования мошенниками банковской инфраструктуры, навести порядок в области регулирования SIP-телефонии, жестко реагировать на нарушения ФЗ в области связи, пересмотреть подходы к расследованию киберпреступлений, организовать постоянный диалог между органами исполнительной власти, банковским сообществом и операторами связи.

ПРИЛОЖЕНИЕ 1. Стенограммы разговора кандидата на устройство в мошеннический call-центр с HR-менеджером

Пример 1:

Кандидат: Алло

HR: Алло. Да, вот так легче будет.

Кандидат: Ира, а можете поподробнее рассказать по скрипту?

HR: Хорошо. Можно ваше имя?

Кандидат: Меня Виталий зовут.

HR: Виталий, очень приятно. Смотрите, работа заключается в том, что Вы работаете через CRM. Работаете с горячей базой клиентов. Вы выполняете обычный обзвон клиентов. Общаетесь. Предлагайте наши услуги — это Сбербанк, если что.

Кандидат: Понял. Подскажите, а что у вас по зарплате?

HR: Зарплата: еженедельные выплаты без задержек. Средняя зарплата новичка 200 - 500 долларов.

Кандидат: Подскажите, а это вообще не опасно? Я просто слышал от друзей…

HR: Нет. Мы уже работаем не первый год на данном рынке. То есть у нас никогда никаких нюансов к нам не было… Алло, меня слышно?

Кандидат: Да – да -да

HR: работаем не первый год. Там уже все нормально, все подвязано. Конфиденциальность мы Вам гарантируем. То есть нас не накрывают. Ничего не делают. У нас собеседование проходит со всеми людьми в несколько этапов, поэтому ну, грубо говоря, к нам некуда подкопаться.

Кандидат: Я понял. А вас там много работает? Большая компания?

HR: Мы работаем на несколько городов. У нас в среднем в каждом офисе по 100 человек сидит.

Кандидат: Понятненько-понятненько.

HR: Хорошо. Смотрите. Давайте сделаем так: если Вы хотите можно встретиться сегодня, либо же завтра в течение дня; пообщаться с Вами более детально, выпить кофе и решить по месту. Если все нормально, можете подъехать потом уже по работе сразу в офис.

Пример 2:

HR: Алло

Кандидат: алло, здравствуйте. Я по поводу работы хотел позвонить узнать у вас…

HR: Вы знаете, что это за сфера?

Кандидат: ну, я хотел узнать вообще, да… Что делать?

HR: смотрите, мы звоним клиентам Банков в РФ и представляемся сотрудниками службы безопасности Банка и обнуляем их счета. Слышали ли Вы за эту сферу? Если да, то подходит она Вам или нет?

Кандидат: Да. Это не опасно?

HR: Нет. Все проплачивается.

Кандидат: а можете рассказать, что по зарплате у вас?

HR: Зарплата выплачивается 4 раза в месяц, в конце каждой рабочей недели на руки. Выплачивается в долларах. Средний доход новичка - это от 150 до 700 долларов за неделю. Ну, в гривнах возьмем… Это от 4 000 до 25 000.

Кандидат: но это точно не опасно? Я вот за это переживаю.

HR: нет, конечно. Не опасно. Я тут уже больше года работаю. Мы сами не местные. Мы с другого города доставлены. Нас сюда пригласили. Сказали, что высокий доход. Касательно безопасности: можете не сомневаться и быть в этом уверены.

Кандидат: зависит как-то зарплата от клиентов? Или какая-то ставка есть минимальная?

HR: да, от общей заведенной суммы. То есть у Вас допустим за неделю, может быть, одна трубка, где было 5 млн. руб., и Вы с нее заработаете 2 500 долларов. А может 3 – 4 закрытые трубки и небольшие суммы это: 200 000 – 500 000 рублей. То есть с них Вы можете заработать долларов 500 – 800. Все зависит от общей заведенной суммы.

Кандидат: Мы же это только по России? По Украине мы не занимаемся?

HR: Да – да.

Кандидат: Сбербанк?

HR: Да

Кандидат: Понятно. У меня ноутбук есть. Мне что-то нужно? Технику там с собой приносить?

HR: Нет – нет. Это все предоставляется, конечно.

Кандидат: Я понял. Ну, а так, наверное, что? Вопросов, наверное, больше нет. Я понял. Хорошо – хорошо. Спасибо большое.

HR: тогда до встречи. До свидания, всего доброго.

ПРИЛОЖЕНИЕ 2. Деятельность call-центра в цифрах

Активный обзвон граждан РФ начался в июле 2021 года. Сотрудниками call-центра совершено за не менее 365 тыс. звонков на 281 тыс. российских номеров телефонов, из которых:

- дольше 1 секунды: 355 тыс.;
- дольше 1 минуты: 49 тыс.;
- дольше 10 минут: 3,8 тыс.

Таким образом, количество пострадавших, по верхней оценке, составляет до 3,8 тыс. человек. Эффективность мошеннических звонков call-центра – 1%.

Режим работы call-центра был стандартным – с понедельника по пятницу, а выходные и праздничные дни мошенническая активность существенно снижалась. Наибольшее количество звонков совершалось по понедельникам, а наименьшее – по воскресеньям. Основные часы работы call-центра – с 8:00 до 17:00, с перерывом на обед (рисунок 54). В среднем в день прозванивалось от 1,5 до 5 тыс. номеров. (рисунок 55)

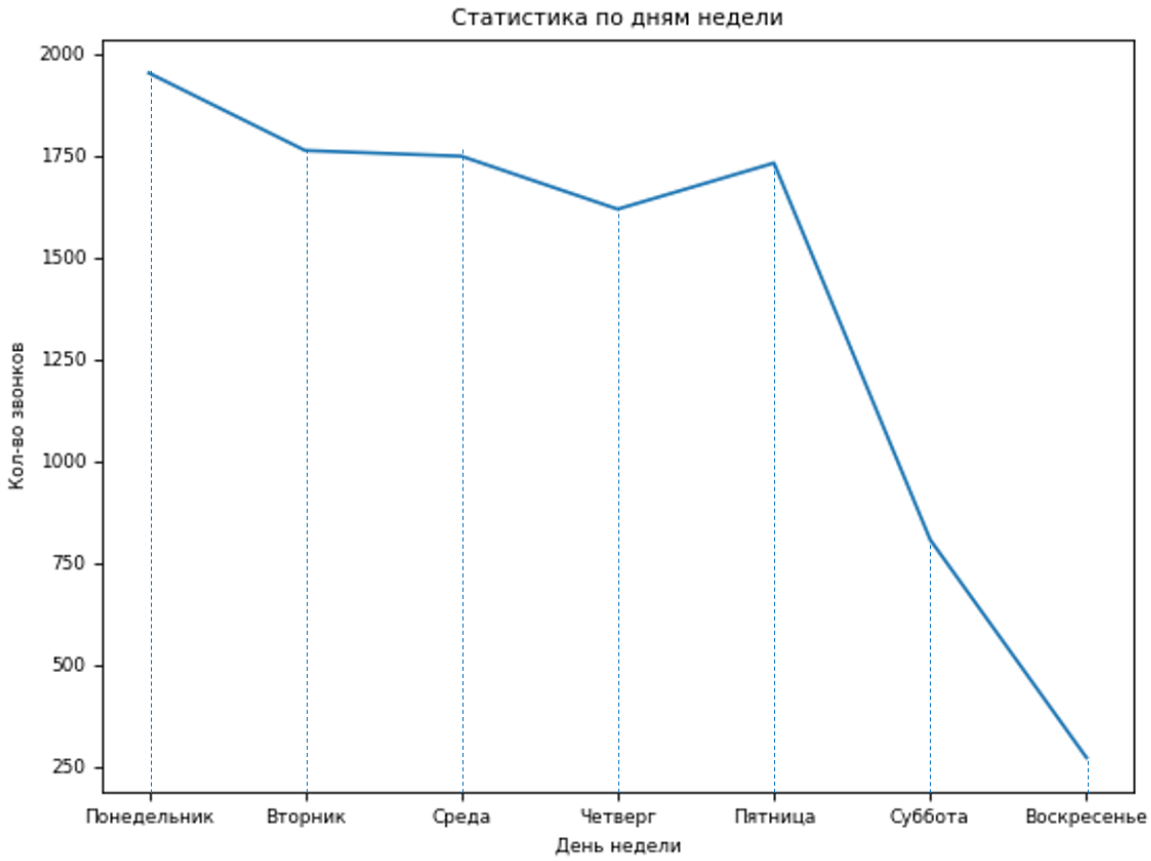


Рисунок 53. Активность работы call-центра по дням недели

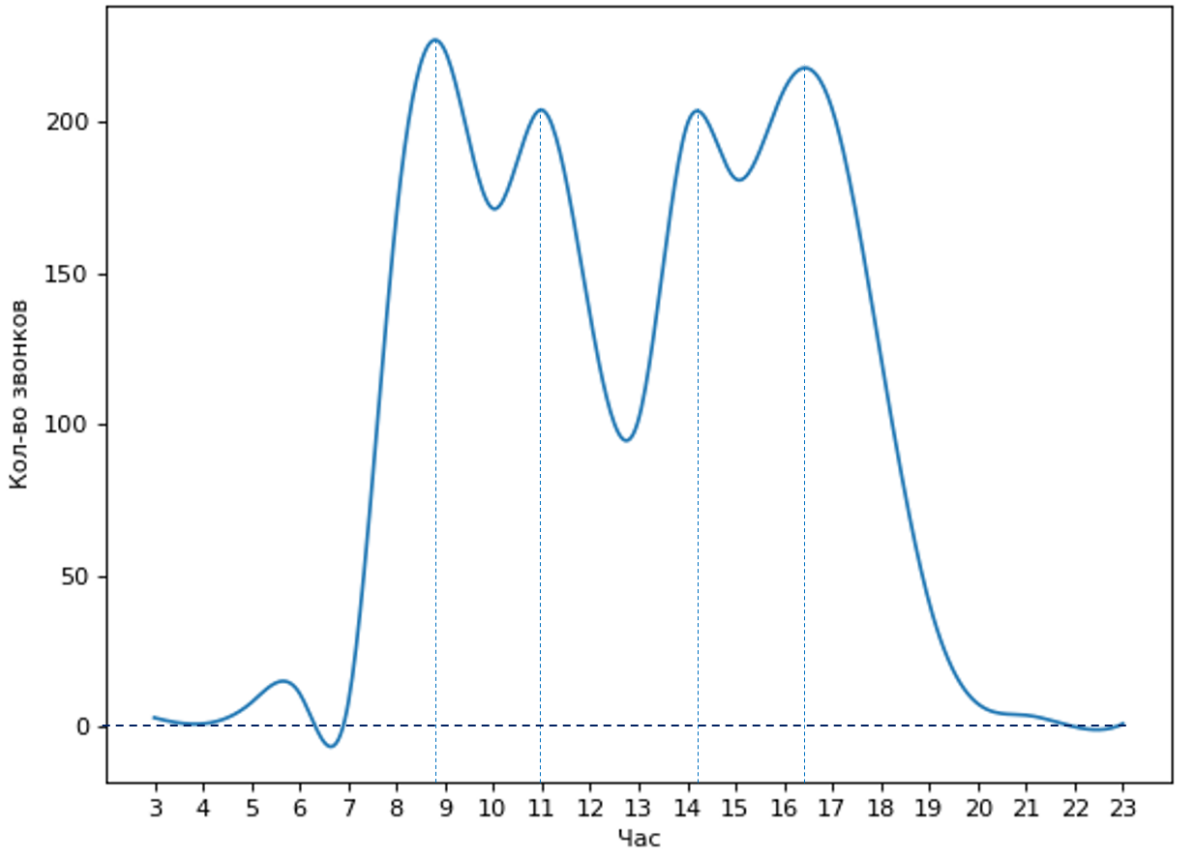


Рисунок 54. Активность call-центра в течении суток (по московскому времени)

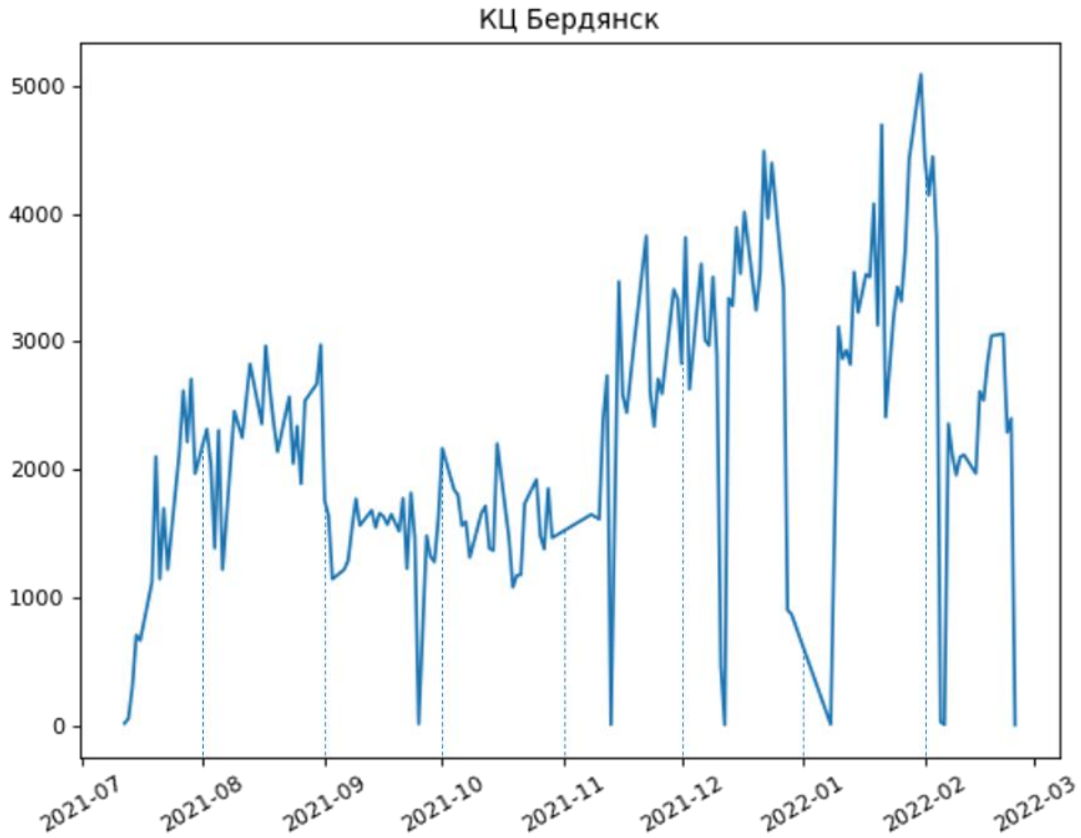


Рисунок 55. Количество звонков за период 07.2021 – 03.2022

Среднее количество звонков:

- в день: 1842;
- в неделю: 6848;
- в месяц: 14518.

Звонки осуществлялись преимущественно на номера телефонов жителей Москвы и Московской области, а также Ленинградской области.

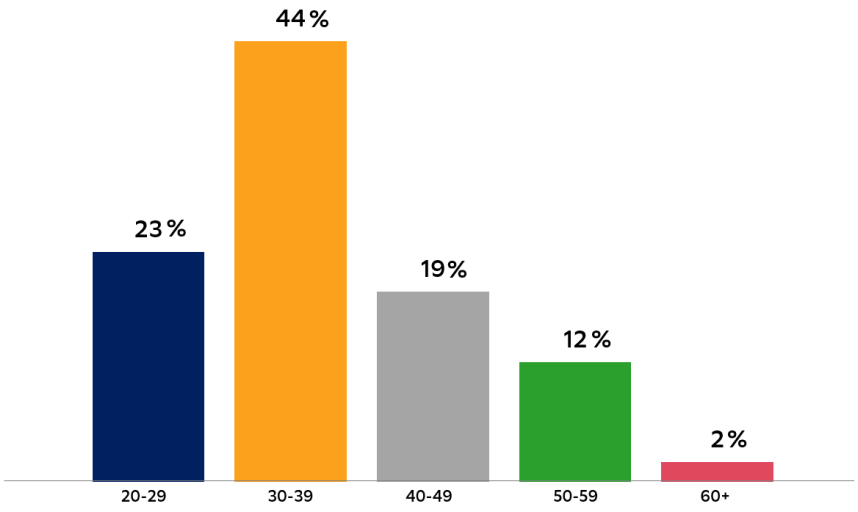


Рисунок 56. Соотношение возрастов жертв в %

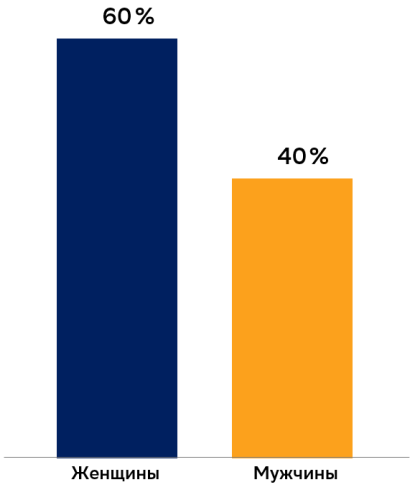


Рисунок 57. Соотношение полов жертв в %

Инфографика на рисунках 56 и 57 показывает, что чаще всего жертвами call-центра становились женщины в возрасте 30-39 лет. Примечательно, что представители старшего поколение в возрасте 60+ вступали в диалог с мошенниками всего в 2% случаев.

ПРИЛОЖЕНИЕ 3. Список bitcoin-кошельков, использовавшихся злоумышленниками.

- 1D6eTZLaUGBStzTyKv81vZ56i1SAPJm883 (общая сумма проведенных денежных средств 0,19691675 BTC (7,579.52$) – курс здесь и далее указан на момент совершения операций);
- 1L5NXnQCgH9VQ6ofAnDYX9Z1zhbcTQBF4m (общая сумма проведенных денежных средств 0,021181 BTC (751.86$));
- 1P3qjcW1RdqYzVSCiiZWKVuZcVhRSYMgWy (общая сумма проведенных денежных средств 0,004179 BTC (156.47$));
- 18jjTHhYQQUYgZJ1j6hZxwAVqyhkxg6PE (общая сумма проведенных денежных средств 0,01250842 BTC (433.42$));
- bc1qud5sdld2gun689rsnhmncl7g6zrxgd8mqqy3am (общая сумма проведенных денежных средств 0,01901405 BTC (715.90$));
- bc1qzk5d66fmra58lzxmzezhxpu4hz5q8yggs7w7hz (общая сумма проведенных денежных средств 0,32887382 BTC (12,957.63$));
- bc1qgnhv7zvj73ualy26t3vamcw6fha9f8yz2675rx (общая сумма проведенных денежных средств 0,24887021 BTC (8,329.19$)).
- bc1q882xa0qu4f9fhtka9xr6d8apl6zevzvv80s8ss (общая сумма проведенных денежных средств 0.11495100 BTC (2 213,01 $)).
- bc1quu3phd2fkjt9p287z6ut9v5yalnz3xrn3nqryz (общая сумма проведенных денежных средств 0.02763026 BTC (531,48 $)).
- bc1q2kfyrg07jk99ehx422jzvj3vhu2k5kr3udkwtc (общая сумма проведенных денежных средств 0.06455094 BTC (1 242,57 $)).
- bc1qv3wf936pc55e4ct3g54t400f8auvjhawegdewz (общая сумма проведенных денежных средств 0.02318152 BTC (446,55 $)).
- bc1q2fc7fh0ntayvlwx7mz7ax2yyq8tk9h4ml77msr (общая сумма проведенных денежных средств 0.02570747 BTC (495,14 $)).
- bc1qgeqgjuuldsfaxcxktdrvzxmhg7mewa8feskunx (общая сумма проведенных денежных средств 0.02317209 BTC (446,30 $)).
- bc1q5exywxyredhygvzm94zj4yz3hm860pqj2mcjsm (общая сумма проведенных денежных средств 0.00136393 BTC (26,27 $)).
- bc1qfuvv4f2uv229tz258xwtsl3v4mu9hr6tua777n (общая сумма проведенных денежных средств 0.00351698 BTC (67,80 $)).

- bc1qpy9xn5sc44y62xx39n5cgjhdw2q4pp2wtksnuk (общая сумма проведенных денежных средств 0.07103632 BTC (1 369,33 $)).
- bc1qysueckk0cqaylgxc33rw8lsdn0juuey7vn8dzk (общая сумма проведенных денежных средств 0.30893107 BTC (5 950,13 $)).
- bc1qq05akczszzzughyvzkrul389k9nuls0zq5xpsl (общая сумма проведенных денежных средств 0.06169890 BTC (1 188,34 $)).
- bc1qv2tsxtt6d97580ug4ht225fnyxs6tet8q79hqp (общая сумма проведенных денежных средств 0.03000000 BTC (577,80 $)).
- bc1qaz8p26uzf4aynnhz4myesa3u7cnq3nkh0aqrct (общая сумма проведенных денежных средств 1.84887797 BTC (35 609,26 $)).
- bc1qjnh40taejygnd24jg4xruwga3vcw5mrx8qcplu (общая сумма проведенных денежных средств 0.13425886 BTC (2 585,82 $)).
- bc1qxrfaq8hcqwafwqyspcczsvctz8wnqrkxd5vene (общая сумма проведенных денежных средств 1.01778734 BTC (19 602,51 $)).
- bc1qnwjxvq0wcjrh2cpv4sp8dx382q04qnjnqps74h (общая сумма проведенных денежных средств 0.21915712 BTC (4 220,95 $)).
- bc1qyvgc32g4nrn084v00nznp0w3djevehxqm3e98r (общая сумма проведенных денежных средств 0.12742240 BTC (2 454,22 $)).
- bc1qq3ha0e97g7lm5u46fpngfj4td8s4d3hdvc30ps (общая сумма проведенных денежных средств 0.00862995 BTC (166,22 $)).
- bc1qn4tly9ezrgpa8fjxd75qydtfy5v6ldephk3cfu (общая сумма проведенных денежных средств 0.05721531 BTC (1 101,72 $)).
- bc1q5ne7ynnuevuuq5va57zn7u48xuqph7r0e9ds08 (общая сумма проведенных денежных средств 0.00796128 BTC (153,30 $)).
- bc1q7pwcdzwvchnee3lh99m0dp9tve0jus0ntrzua0 (общая сумма проведенных денежных средств 0.02342248 BTC (451,02 $)).
- bc1qc5ay2mf7smlfyww263xgpldzn8e5fv5v7hz6re (общая сумма проведенных денежных средств 0.00664874 BTC (128,03 $)).
- bc1q44t7tqrndrva4fr8gg88rrx2jxuwxv468sflvc (общая сумма проведенных денежных средств 0.05640368 BTC (1 086,09 $)).
- bc1qt4tya8xwlfnael3xq7z0ftwlp7940hdf5e0250 (общая сумма проведенных денежных средств 0.00805251 BTC (155,06 $)).
- bc1q4u50ldujmwyval95h8z0r7wy6mqrppnylvkpf4 (общая сумма проведенных денежных средств 0.02763026 BTC (532,04 $)).