ПРАВИТЕЛЬСТВО
НИЖЕГОРОДСКОЙ
ОБЛАСТИ

Дистанционные преступления и их влияние на террористическую угрозу

Методические материалы

Авторы:
Силантьев Р.А., Филиппов Д.В.,
Василишина О.М., Громова А.Н.

Управление делами
Администрации
Волгоградской области

Нижний Новгород
2025

УДК 323.28:004.7
ББК 66.4(0),304с51
Д48

Автор идеи **Павел Константинович Карасев**

Д48 **Дистанционные преступления и их влияние на террористическую угрозу:** Методические материалы / Авторы Р.А. Силантьев, Д.В. Филиппов, О.М. Василишина, А.Н. Громова – Нижний Новгород, 2025. – 108 с.; илл.

ISBN 978-5-6048841-5-7

Методические материалы представляют собой комплексную научно-методическую разработку, посвященную анализу феномена дистанционных преступлений и их трансформации в инструмент гибридной войны и террористической деятельности. Основное содержание сосредоточено на механизмах психологического манипулирования (социальной инженерии), используемых для вовлечения граждан в противоправную, в том числе диверсионно-террористическую, деятельность.

Особое внимание уделено криминологическому и виктимологическому анализу, формированию социально-психологического портрета потенциальной жертвы. Представлены практические рекомендации по противодействию данной угрозе, направленные на пресечение деятельности низовых звеньев преступных сетей, купирование детерминант преступности и формирование у населения навыков психологической устойчивости к манипуляциям.

Методические материалы предназначены для сотрудников правоохранительных органов и специальных служб, специалистов в области корпоративной и информационной безопасности. Издание будет полезно руководителям и сотрудникам сферы образования и молодежной политики, психологам и всем, кто занимается вопросами профилактики экстремизма, терроризма и деструктивного поведения в цифровой среде.

18+

УДК 323.28:004.7
ББК 66.4(0),304с51

ISBN 978-5-6048841-5-7

© Правительство Нижегородской области, 2025

ОГЛАВЛЕНИЕ

Предисловие 4

Введение 7

Глава I. Дистанционные преступления в системе современной противоправной деятельности 10

I.1. Количественные показатели дистанционных преступлений 10

I.2. Технологические аспекты организации дистанционных преступлений 18

I.3. Целевые аудитории дистанционных преступлений 27

Глава II. Виды дистанционных преступлений 41

II.1. Мошенничество 41

II.2. Вовлечение в преступную деятельность 62

II.3.Доведение до самоубийства 71

II.4.Феномен «биодронов» 78

Глава III. Направления деятельности по профилактике и противодействию дистанционным преступлениям 85

III.1. Нормативно-правовые и технологические направления противодействия дистанционным преступлениям) 85

III.2. Профилактика дистанционных преступлений 99

Заключение 104

Предисловие

Развитие информационно-коммуникационных технологий стало, своего рода, триггером миграции мошеннических схем в пространство интернета и телефонии. Исключение формата общения «тет-а-тет», развитие технологий создания дипфейков, совершенствование навыков социальной инженерии: все эти процессы существенно поспособствовали уходу мошенников в социальные сети и мессенджеры.

Российская Федерация оказалась одним из государств, где масштабы дистанционного мошенничества очень быстро стали существенными. Следует вдуматься в следующие цифры. Только за одну неделю июля 2025 года, в период с 14 по 20 июля, жители Нижегородской области стали жертвами 76 мошеннических афер, потеряв более 54 млн рублей! Порядка 11-ти мошенничеств в сутки! В федеральном масштабе аналогичные показатели просто колоссальны: по оценке специалистов Сбербанка, ущерб от телефонного мошенничества в 2024 году составил не менее 295 млрд рублей!

Рынок кибермошенничества, телефонного мошенничества растет во всём мире. Наибольшие абсолютные показали числа обманутых граждан и объема украденных денег приходятся на Соединённые Штаты Америки. На второй позиции находится Китайская Народная Республика, чьи власти, несмотря на все рычаги контроля над информационно-коммуникационным пространством, не могут полностью защитить своих граждан.

Однако, у России есть своя, к сожалению, негативная специфика. По основным относительным показателям (процент звонков или писем мошенников, процент обманутых россиян в пересчёте на всё население) Российская Федерация является лидером. Это напрямую связано с условиями гибридного противостояния, в котором оказалось государство. Если в США, Китае, странах Западной Европы всё ограничивается именно мошенничеством (североамериканцы,

например, очень любят финансовые интернет-пирамиды), то есть кражей денежных средств или получением доступа к ним, то в Российской Федерации мошенничество – это только одно из направлений работы с россиянами.

Как правило, обманывают россиян на первом этапе, чтобы в дальнейшем использовать данный факт для вовлечения их в противоправную деятельность: сбор разведывательных данных и фиксацию последствий ударов БПЛА, совершение акций экстремистского и террористического характера. Но и этим всё не ограничивается. Масштабы дистанционного мошенничества по отношению к россиянам вызывают у последних естественные и обоснованные претензии к силовым органам, структурам безопасности, властным институтам в целом. В контексте вопроса «почему полиция/ФСБ/власть нас не защищает?» формируются недоверие официальным политическим институтам и антивластные настроения.

Относительные высокие показатели мошенничества в отношении россиян обусловлены тем, что в Российской Федерации за мошенниками стоят и спецслужбы стран Запада, и представители несистемной оппозиции. В качестве примера можно привести кейс с отечественным мессенджером «MAX», когда большое количество медийных ресурсов с различных площадок распространяли негативные отзывы и характеристики о данном отечественном продукте. Известие о первом мошенничестве в «MAX» эта же сетка медиаресурсов публиковала и репостила буквально с радостью. Однако, Центр безопасности мессенджера «MAX» в течение суток вычислил и мошенническую схему, и самого мошенника, и передал информацию в полицию. Перевод был оперативно заблокирован на счёте мошенника, которого объявили в розыск, жертва получила возможность вернуть украденные денежные средства. Налицо прямая попытка сорвать внедрение инструмента, способного существенно ограничить возможности мошенников и защитить простых россиян.

Угрозы, формируемые дистанционной преступностью в современных условиях гибридного противостояния, требуют максимально возможного реагирования по всем направлениям. Необходимо развивать научные изыскания, совершенствовать законодательную базу и правоприменительную деятельность. Необходимо изучать целевые аудитории мошенников, технологии, методы и приёмы обмана россиян. Крайне необходимо развивать и совершенствовать профилактическую деятельность.

Представленные методические материалы никоим образом не стоит воспринимать как панацею от всех бед, как материал, изучение которого и применение на практике способно полностью решить все проблемы. Скорее это серьёзные изыскания, которые могут и должны быть приняты во внимание в практической сфере, но, помимо этого, должны стать этапом в системном взаимодействии представителей науки, сотрудников органов безопасности и охраны порядка, чиновников всех уровней. Обеспечение национальной безопасности Российской Федерации, личной безопасности россиян – это наше общее дело!

Введение

События украинского Евромайдана в 2014 года ознаменовали переход информационно-психологического противоборства в новую, активную фазу: украинские спецслужбы объявили войну России и запустили целую линейку информационно-психологических операций. Для этого была использована сеть из четырех Центров информационно-психологических операций (ЦИПСО) в составе Вооруженных сил Украины, которые были созданы еще в 2004 году. Получив значительное финансирование и расширенные полномочия, эти подразделения, укомплектованные специалистами в области информационных войн, развернули масштабную деятельность против Российской Федерации.

Первоначально активность ЦИПСО ассоциировалась преимущественно с распространением дезинформации. Однако вскоре их тактика эволюционировала, приобретя новую, криминально-экономическую направленность. Именно с этого периода в России начался экспоненциальный рост дистанционных мошенничеств, совершаемых с использованием телефонной связи. Под предлогом защиты сбережений от мнимых угроз злоумышленники, представлявшиеся сотрудниками банков и правоохранительных органов, начали массово похищать средства граждан.

Изначальные версии о причастности к этим схемам исключительно российских криминальных структур, в том числе действующих из мест лишения свободы, не нашли полного подтверждения. Как показала практика, данный вид преступной деятельности был поставлен на поток именно на территории Украины при непосредственном участии и под контролем местных спецслужб.

Примерно в 2015 году на Украине, а затем в Польше и ряде других стран были созданы сотни колл-центров, к работе в которых были привлечены сотни тысяч человек. Они получили

базы данных, полученные в результате утечек из банков, служб доставки и иных структур, а также специальные регулярно обновляемые методические рекомендации по манипуляции людьми, составленные опытными психологами.

Эта криминальная индустрия вовлекла в свою орбиту и граждан России, которым отводилась роль низшего, но критически важного звена — так называемых «дропов». Их функции заключаются в приеме и обналичивании похищенных средств, а также предоставлении своих банковских счетов для транзита денег жертв.

Звонки, ежегодное количество которых уже достигло одного миллиарда (в некоторые периоды до 20 млн. в день), делаются от имени банковских операторов, сотрудников служб безопасности банков, представителей МВД, СКР и ФСБ. Применяемые схемы хищения средств постоянно модифицируются, но в целом сводятся к требованию перевести все деньги на «безопасный» счет или же обналичить их с последующей передачей «дропу».

Есть основания полагать, что подобного рода звонками охвачено уже почти все взрослое население страны. Ежегодные убытки от такого мошенничества оцениваются в сотни миллиардов рублей.

Число жертв вышеприведенных схем уже превышает миллион человек (по некоторым оценкам до 10 млн.), преимущественно пожилого возраста. Среди пострадавших можно встретить и тех людей, которые, казалось, по долгу службы не должны становиться жертвами подобных манипуляций - высокопоставленных чиновников, военнослужащих, правоохранителей.

Со временем цели и методы злоумышленников претерпели качественную трансформацию, выйдя за рамки обычного мошенничества. К хищению средств добавились элементы шантажа и прямого вовлечения в преступную деятельность. Граждан, уже пострадавших от мошенников, начали

принуждать к переводу оставшихся средств под угрозой обвинения в государственной измене и финансировании ВСУ. Более того, зафиксированы многочисленные случаи, когда жертв психологического воздействия склоняли к совершению диверсионно-террористических актов, таких как поджоги банкоматов, релейных шкафов и объектов военной инфраструктуры.

Проблема приобрела такой масштаб, что на высшем государственном уровне телефонное мошенничество было охарактеризовано как элемент государственной политики Украины, направленной на дестабилизацию обстановки в России. Показательно, что в первые месяцы после начала Специальной военной операции правоохранительными органами отмечалось резкое, почти полное прекращение данного вида преступлений, что косвенно указывает на их централизованное управление из-за рубежа.

В феврале 2025 года Президент России Владимир Путин дал поручения Роскомнадзору и другим ведомствам обратить внимание на проблему мошеннических звонков с территории Украины. Об этом глава государства заявил на заседании Совета при президенте РФ по развитию гражданского общества и правам человека (СПЧ). Президент добавил, что телефонное мошенничество на Украине возведено в ранг госполитики как одна из линий атак на Россию.

«Это делают часто государственные органы или структуры, которые находятся под государственным украинским контролем», — заявил он[1].

Настоящее пособие призвано системно рассмотреть феномен дистанционных преступлений, выходя за рамки исключительно мошенничества и анализируя их как комплексную угрозу, тесно связанную с современными вызовами национальной безопасности, включая террористическую деятельность.

1 https://tass.ru/ekonomika/23087757

Глава I. Дистанционные преступления в системе современной противоправной деятельности

I.1. Количественные показатели дистанционных преступлений

Дистанционные преступления к 2025 году стали самым распространенным видом преступной деятельности в России. Злоумышленники охватили своими звонками или текстовыми сообщениями большую часть граждан нашей страны, имеющих смартфоны. Количество пострадавших может приближаться к 15% населения, хотя соответствующие заявления в правоохранительные органы подали только порядка миллиона граждан. Исходя из этих заявлений сотрудники МВД могут примерно подсчитать объем потерь.

«В истекшем (2024 году) году зарегистрировано более 765 тыс. Из которых более 494 тыс. дистанционных хищений. Ущерб от этих преступлений составил более 203 млрд рублей.

За 4 месяца текущего (2025 года) года зарегистрировано более 247 тыс. IT-преступлений. Основная доля этих преступлений по-прежнему – дистанционные мошенничества, которых более 154 тыс.

Ущерб составил 64 млрд рублей и эта сумма на 17% процентов больше аналогичного периода прошлого года (53 млрд.).

Как мы понимаем, большая часть похищенных денежных средств выведена из юрисдикции Российской Федерации», - заявил на Петербургском международном юридическом форуме 19 мая 2025 года заместитель начальника Следственного департамента МВД России генерал-майор юстиции Данил Филиппов, курирующий борьбу с дистанционными преступлениями[2].

2 https://www.interfax.ru/russia/1026404

Ранее он уточнил, что «в 2023 г. зарегистрировано 677 тыс. преступлений, совершенных с использованием IT-технологий, из которых более 161 тыс. направлены в суд с обвинительным заключением, привлечено к уголовной ответственности более 105 тыс. лиц. Причиненный потерпевшим ущерб составил 156 млрд рублей».

А вот цитата главы МВД России: «в ходе выступления в мае в Совфеде глава МВД России Владимир Колокольцев отмечал, что ущерб от киберпреступлений в РФ за 2023 год составил 156 миллиардов рублей, пострадали 113 тысяч пенсионеров и семь тысяч несовершеннолетних. Выступая на заседании коллегии МВД, посвященному противодействию IT-преступности, В. Колокольцев заявил, что с 2020 года число посягательств с использованием информационных технологий увеличилось на треть. Сейчас доля дистанционных деяний в общем массиве приближается к 40%.

«В прошлом году от них пострадало полмиллиона человек, из которых практически каждый четвертый - пенсионер. Уже в этом году жертвами различных уловок преступников стали более 40 тысяч граждан преклонного возраста. Существенным является размер причиненного ущерба. Суммарно за 2023-й и четыре месяца текущего года он превысил 210 миллиардов рублей», — сказал он и отметил, что в прошлом и текущем годах фиксируется всплеск фактов неправомерного доступа к компьютерной информации. По его словам, в 2020 году их доля среди дистанционных составов не превышала 1%, сейчас это каждое восьмое IT-преступление»[3].

Действительно, только по официальным данным россияне ежегодно теряют от дистанционного мошенничества сотни миллиардов рублей, а с учетом неизвестных правоохранителям случаев эта сумма может достигать полутриллиона. Как

3 https://www.audit-it.ru/news/finance/1103507.html

показывает практика, потерпевшие не пишут заявления по трем основным причинам:

1. Считают сумму ущерба незначительной.
2. Считают сумму ущерба слишком значительной и опасаются отвечать на вопросы о происхождении похищенных средств.
3. Не верят в возможность компенсации потерь и поимки преступников.

Тем не менее, ежедневно в России возбуждается до полутора тысяч уголовных дел по таким эпизодам. Каждый регион ежегодно (за исключение двух самых малолюдных) несет потери от 2 до 56 миллиардов рублей. В 2025 году наибольший прирост регистрации мошенничеств отмечался в г. Санкт-Петербурге, Камчатском, Хабаровском краях, Сахалинской, Московской областей, в то время как положительная динамика наблюдалась в республиках Дагестан, Адыгея, РСО Алания, Чукотском АО и г. Москве.

С целью определить масштаб проблемы стали проводится опросы. «Самый популярный вид мошенничества, с которым сталкивались россияне — телефонное. Таковы данные исследования, проведенного Ozon. С телефонным мошенничеством столкнулись 79% опрошенных. С фейковыми сотрудниками служб и учреждений — 56% опрошенных, а с предложениями о работе и подработках — 33%.

У 14% респондентов мошенникам удалось украсть средства:

- в 82% случаев кража не превышала 100 тыс. рублей;
- 26% потеряли до 5 тыс. рублей;
- 18% опрошенных отдали мошенникам суммы свыше 100 тыс. рублей.

По данным опроса, средний возраст пострадавших от аферистов составляет 65 лет. Чаще всего мошенники звонили по мобильному телефону (78%), в остальных случаях использовали СМС, мессенджеры Telegram или

WhatsApp. В каждом втором случае аферисты хотели обманом узнать конфиденциальные данные, SMS-код или пароль (в 49% случаев). В каждом третьем (34%) — убеждали либо перевести деньги на другой счет, либо перейти по ссылке (опрос проводился в декабре 2024 года среди россиян старше 18 лет с использованием онлайн-анкеты. Всего в исследовании приняли участие 1000 респондентов из крупнейших городов России)»[4].

Каждый шестой россиянин когда-либо становился жертвой мошенников, лишаясь денег или имущества. В опросе сервиса по поиску высокооплачиваемой работы SuperJob приняли участие 1600 экономически активных граждан из всех регионов страны. Мошеннические схемы становятся все более изощренными: современные технологии позволяют воровать и использовать в преступных целях биометрические данные. 15% опрошенных россиян рассказали, что звонки от мошенников поступают им ежедневно, каждому четвертому (23%) звонят несколько раз в неделю, столько же участников опроса принимают подозрительные звонки несколько раз в месяц. Только каждый седьмой респондент утверждает, что ни разу не сталкивался с подозрительными звонками. Из комментариев россиян следует, что звонящие с подозрительных номеров чаще всего представляются сотрудниками операторов связи, банков, полиции, ФСБ, прокуратуры, Госуслуг, Почты России, Горгаза и других жилищных сервисов.1 из 6 россиян приходилось попадаться на уловки мошенников и терять деньги или имущество: 12% — однократно, 5% — несколько раз. Больше жертв мошеннических схем — среди россиян с доходом от 100 тысяч рублей в месяц (19%)»[5].

4 https://lapsha.media/carefully/moshenniki-starshee-pokolenie/

5 https://www.superjob.ru/research/articles/115115/kazhdyj-shestoj-rossiyanin-popadalsya-na-ulovki-telefonnyh-moshennikov/

«По данным опроса Фонда «Общественное мнение» (ФОМ), каждый одиннадцатый россиянин признался: он терял деньги из-за телефонных аферистов. Это не просто цифры — это миллионы пострадавших. Что ещё выяснилось:

— 73% россиян за последний год получали звонки от мошенников;
— Только 18% избежали такой атаки;
— Ещё 9% затруднились ответить.

По данным ФОМ, более половины россиянин (58%) уверены, что смогли бы в случае такого звонка распознать признаки телефонного мошенничества, более четверти респондентов (28%) в этом сомневаются, а каждый седьмой (14%) не знает, что сказать по данному поводу. Согласно опросу, почти каждый второй россиянин (48%) считает, что в настоящее время есть эффективные методы борьбы с телефонными мошенниками, около трети респондентов (30%) в этом сомневаются, оставшиеся 22% опрошенных затрудняются составить свое мнение. Опрос проводился 11-13 апреля 2025 года среди 1500 респондентов в возрасте от 18 лет в 97 населенных пунктах РФ, в 51 регионе»[6].

А вот типичный релиз прокуратуры Тюменской области: "За минувшую неделю *(первая неделя июня 2025 года)* от рук телефонных и интернет-мошенников пострадал 91 житель региона. Общая сумма похищенных денежных средств превысила 26 миллионов рублей. За прошедшую неделю максимальный ущерб от мошеннических действий составил 3,3 миллиона рублей»[7].

А вот как оценивает ситуацию член Совета при президенте РФ по развитию гражданского общества, известный специалист по кибербезопасности Игорь Ашманов: «Украинские мошенники ежедневно крадут у россиян 1

6 https://www.interfax.ru/russia/1028070
7 https://ura.news/news/1052942607

млрд рублей». По словам Ашманова, надо «говорить про абсолютные цифры, их надо называть - это сотни миллиардов рублей в год, которые растут ежегодно на 20-30%». Он отметил, что это не просто хищения, а информационная атака другого государства на Россию. «Телефонные мошенники с Украины управляются Службой безопасности Украины и американскими инструкторами, то есть это не какие-то частные мошенники, которые, как когда-то говорили, сидят в тюрьмах», - сказал Ашманов.

По его словам, в этой сети работают 50-70 тыс. человек. "Это можно легко подсчитать, потому что 20 млн звонков в день люди получают. [Каждый мошенник] совершает 300-400 звонков. То есть работают 50 тыс. человек минимум", - сказал Ашманов. Он отметил, что все эти люди нанимаются открыто через кадровые агентства»[8].

По данным из открытых источников представляется возможным составить рейтинг наиболее крупных хищений денежных средств и иного имущества в результате дистанционного мошенничества:

1. Более 421 млн. - бывший руководитель Корпорации развития Самарской области Ольга Серова[9].
2. 317 млн. - певица Лариса Долина[10].
3. 200 млн - сын московского предпринимателя Ильи Гурова Михаил[11].
4. 148 млн. - московский пенсионер[12].
5. 121 млн. - жительница города Тольятти[13].

8 https://t.me/banksta/67100
9 https://life.ru/p/1721375
10 https://ria.ru/20250416/dolina-2011559499.html
11 https://msk-news.net/society/2025/03/20/633427.html
12 https://ria.ru/20250520/pensioner-2018040233.html
13 https://www.ntv.ru/novosti/2879699/

6. Более 87 млн. - бывший начальник Приволжской железной дороги Александр Храпатый[14].
7. 85 млн. - начальник отдела экономической безопасности Национального медицинского исследовательского центра онкологии имени Н. Н. Блохина[15].
8. 83 млн. - московский пенсионер[16].
9. 74 млн. - дама-нотариус из Москвы[17].
10. 65 млн. - сын гендиректора «Газпром-медиа» и экс-главы Роскомнадзора Николай Жаров[18].
11. 64 млн. - пенсионерка из Москвы[19].
12. Более 62 млн. - советник генерального директора МАК «Вымпел» Александр Рахманов[20].
13. 60 млн. - генерал КГБ в отставке Юрий Яровенко[21].
14. 60 млн. - москвич[22].
15. 53 млн. - профессор МГУ Борис Бояринцев[23].
16. 50 млн. - дочь депутата Госдумы IV созыва Анна Красильникова[24].

---

14 https://www.business-vector.info/eks_glava_privzhd_otdal_moshennikam_bolee_80_mln_i_prigotovil_5_banok_chernoy_ikry/
15 https://news.rambler.ru/incidents/53807296-baza-moshenniki-obmanuli-sotrudnika-onkotsentra-imeni-blohina-na-85-millionov/
16 https://epp.genproc.gov.ru/web/proc_77/mass-media/news/reg-news?item=96909074
17 https://iznanka.news/articles/Proisshestviya/Notarius-iz-Moskvy-perevela-moshennikam-74-milliona-rubley.html
18 https://lenta.ru/news/2025/02/10/syn-byvshego-glavy-roskomnadzora-otdal-moshennikam-65-millionov-rubley-i-kollektsiyu-chasov/
19 https://www.rbc.ru/society/26/07/2025/68849ec89a79475a77c851e8
20 https://radio1.ru/news/obschestvo/moshenniki-ukrali-u-sovetnika-generalnogo-direktora-mak-vimpel-bolee-62-millionov-rublei/
21 https://www.gazeta.ru/social/news/2024/09/08/23874985.shtml
22 https://epp.genproc.gov.ru/web/proc_77/mass-media/news?item=96008452
23 https://www.gazeta.ru/social/2025/05/27/21109424.shtml
24 https://www.gazeta.ru/social/news/2025/02/06/25019330.shtml

17. 50 млн. - баскетболистка студенческой команды МГАФК[25].
18. 45 млн. - драматург и публицист Эдвард Радзинский[26].
19. Более 44 млн. - 62-летняя пенсионерка из Амурской области[27].
20. 43 млн. - 90-летний изобретатель из Санкт-Петербурга[28].
21. 41 млн. - экс-помощница президента инвестиционной компании Millhouse[29].
22. 40 млн. - советник заместителя гендиректора одной из структур «Роскосмоса» Андрей Петренко[30].
23. 38 млн. - жительница Иркутска[31].
24. 37 млн. - жительница Москвы[32].
25. 35 млн. - вдова генерала из Москвы Лариса Купреева[33].

Дистанционные преступления не ограничиваются только дистанционным хищением средств. Граждан России активно вовлекают и в другие преступные схемы — предлагают стать помощниками мошенников дропперами, операторами симбоксов — сотни тысяч случаев, совершить диверсионный или террористический акт (сотни случаев). Известны случаи дистанционного доведения до самоубийства (десятки случаев),

25 https://www.sport-express.ru/basketball/reviews/moshenniki-obmanuli-basketbolistku-mgafk-na-50-millionov-rubley-podrobnosti-2277948/
26 https://78.ru/articles/2024-09-23/moshenniki-ukrali-45-mln-a-sin-stal-inoagentom-kak-zhivet-edvard-radzinskii-posle-amnistii
27 https://rg.ru/2024/01/27/v-amurskoj-oblasti-pensionerka-perechislila-moshennikam-bolee-44-mln-rublej.html
28 https://www.fontanka.ru/2025/05/29/75519017/
29 https://finance.rambler.ru/money/54502862-baza-eks-sotrudnitsa-millhouse-otdala-moshennikam-41-mln-posle-zvonka-iz-fsb/
30 https://ura.news/news/1052784073
31 https://www.irk.ru/news/20250515/cheater/
32 https://lenta.ru/news/2025/04/02/zhitelnitsa-moskvy-otdala-moshennikam-dve-kvartiry/
33 https://www.ntv.ru/novosti/2823820/

а также преобразования жертвы мошеннических действий в биодрона, то есть одновременно потерпевшего и преступника (сотни случаев).

I.2. Технологические аспекты организации дистанционных преступлений

Дистанционные преступления в современной России в подавляющем большинстве совершаются гражданами Украины, которые при помощи спецслужб этой страны создали сеть особого рода ОПГ - так называемых коллцентров. По данным «Сбера», эта сеть насчитывает до 1000 такого рода преступных групп, из которых около 300 базируется в городе Днепре (Днепропетровске) — мировой «столице» мошенников[34].

Специалисты «Сбера» также утверждают, что 92% звонков преступников направлены на Россию, а оставшиеся 8% получают жители других стран, преимущественно Польши, Германии и Казахстана. Впрочем, страдают и многие другие страны — особенно Канада и Израиль, где проживает много русскоязычных. Например, летом 2025 года украинские телефонные мошенники воспользовались двухнедельным конфликтом между Израилем и Ираном и украли 80 млн. долларов у израильтян, представляясь сотрудниками Моссада и обещая защиту от иранских ракет.

Часть украинских колл-центров (более 150) действуют по иностранной франшизе. «Каждый пятый мошеннический колл-центр на Украине работает по модели франшизы и управляется из Нидерландов и Германии», - заявил зампред правления Сбербанка Станислав Кузнецов, выступая на 32-й сессии Комиссии ООН по предупреждению преступности и уголовному правосудию. Действительно, основные

34 https://ria.ru/20230524/moshenniki-1873965097.html

мошеннические схемы были разработаны в США и Западной Европе, там же возникли и крупные компании, получающие доход таким образом.

После освобождения Запорожской и Херсонской областей в 2022 году российские правоохранители получили доступ ко внутренним материалам ряда колл-центров, которые находились на их территории, что позволило лучше понять механизмы их работы.

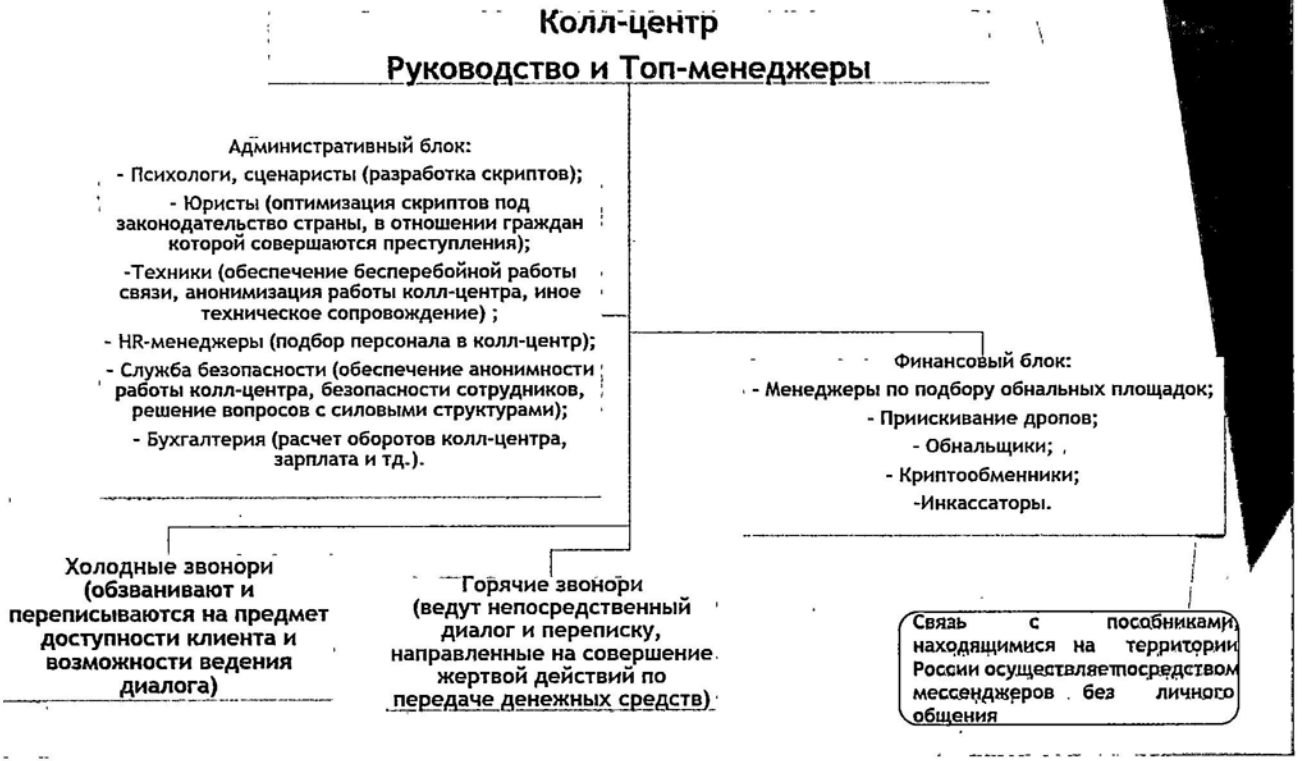
Колл-центры покупают украденные базы данных, в которые попали личные данные почти всех граждан России. Особую ценность для них представляют электронные трудовые книжки, которые позволяют реализовывать двухуровневую схему «звонок/смс-сообщение от действующего или бывшего руководителя с предупреждением о проверке ФСБ, затем звонок от «сотрудника ФСБ». Специальные программы позволяют колл-центрам генерировать документы и удостоверения любых организаций, а также подменять голоса и видеоизображения (проблема дипфейков).

Для подмены номеров мошенники вербуют сообщников на тех территориях, которые обзванивают, и развертывают сеть специального оборудования — сим-боксов, которые насыщаются сотнями местных сим-карт. Это позволяет подменять зарубежные номера не просто на российские, а на российские с местным префиксом. Впрочем, успешные меры борьбы с сим-боксами и введенные ограничения на покупку сим-карт привели к тому, что большая часть звонков или сообщения поступает россиянам через мессенджеры. Ранее ежедневно фиксировалось до 20 млн подобных звонков и смс-сообщений, к середине 2025 года их количество сократилось до 5-6 млн. При этом, по данным МВД в 2025 году ежедневного фиксировалось от 1000 до 1400 пострадавших россиян.

Сотрудники колл-центров в зависимости от своей квалификации делятся на «звонарей» («звонилок»)

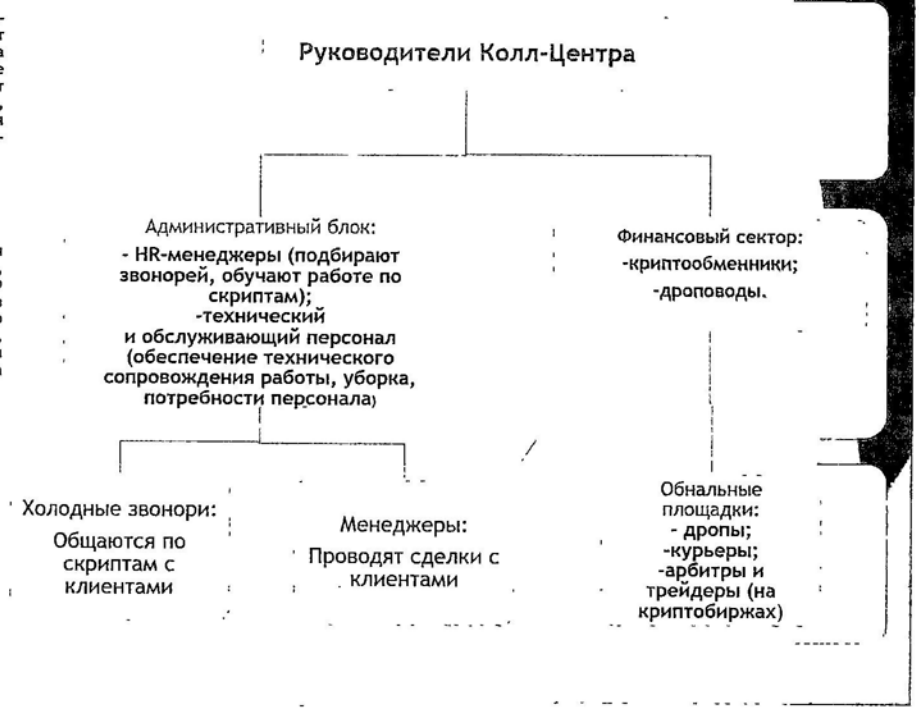
Территориальные подразделения, выявившие и прекратившие работу кол-центров

Структура организаторов колл-центра, находящихся за пределами России



Структура ячейки колл-центра, находящейся на территории России

Как правило назначаются из числа Топ-менеджеров, организация начинает работать по системе франшиза (осведомлены о преступном характере деятельности колл-центра), приискивают номинальных генеральных директоров, фирмы которых используются для придания законности деятельности колл-центра



Сотрудники приискиваются административным блоком колл-центра, находящегося за пределами РФ посредством интернет ресурсов (административный блок не осведомлен о преступном характере работы колл-центра, финансовый сектор - осведомлены организаторы, как правило находятся за границей)

Неосведомлённые о преступном характере своих действий, не знают организаторов

Что узнали о деятельности колл-центров

- Стоимость создания «под ключ» колл-центра варьируется от 500.000 до [illegible] США.
- Как правило колл-центры открываются по франшизе.
- Колл-центры работают на территории Российской Федерации, однако [illegible] деятельность направленна на хищение денежных средств иностранных граждан.
- При организации работы колл-центров используются популярные площадки для подбора персонала (hh.ru, авито, работа.ру и др).
- Для аренды помещений используются номинальные юридические образования.
- Расчет с сотрудниками колл-центров осуществляется либо наличными, либо на криптокошельки.
- Организаторы находятся за пределами юрисдикции Российской Федерации.

и «клоузеров» («закрывающих»). Сначала номера потенциальных жертв обрабатывает 1-я линия обзвона – «звонари». Им выдают скрипт, посредством которого они должны выявлять наиболее доверчивых и уязвимых людей. Самые неквалифицированные «звонари» общаются только в письменном виде, выбирая варианты ответов-вопросов из специального списка. Более опытные, для которых ключевым требованием является хорошее знание русского языка, звонят от имени операторов сотовой связи, банков, МФЦ и других.

Когда становится понятно, что человек «попал на удочку», то его переводят на 2-ю линию обзвона – «клоузеров». Если для «звонарей» важно установить первоначальный контакт, то «клоузеры» занимаются уже завершением мошеннической схемы. Они представляются сотрудниками российских спецслужб, обычно ФСБ, и запугивают жертву возбуждением уголовного дела за государственную измену или финансирование терроризма. Если к этому моменту жертва сообщила код от портала Госуслуг, то их работа упрощается — в дело вступает схема с оформлением кредитов и пересылке полученных средств Вооруженным силам Украины. «Клоузеры» этого уровня имеют поставленный командный тон, говорят на чистом русском языке и хорошо представляют себе российские реалии.

В крупных колл-центрах выстроена полноценная иерархия — в них есть служба собственной безопасности, которая наказывает нерадивых сотрудников посредством отправки на фронт, кадровая служба и прочие характерные для законопослушных организаций подразделения.

Украинские СМИ отмечают, что у колл-центров есть свои «крыши» как в правоохранительных органах, так и непосредственно украинской власти. Так, например, даже во время отключения электроэнергии колл-центры обеспечены бесперебойной работой света. В вакансиях отмечается, что работодатели помогут своим работникам решить проблемы

с ТЦК. А облавы на колл-центры связывают не с желанием Киева разобраться с мошенниками, а с конкуренцией между «крышами». Конкурировать есть за что – это один из немногих бизнесов на Украине, который даже в нынешнее время приносит огромную прибыль.

«RT выяснил, как работает украинский центр телефонных мошенников, которые по указке кураторов вымогают у россиян деньги. Наш корреспондент под видом соискателя откликнулся на вакансию киевского центра, где узнал о «новом алгоритме разводки», внедряемом среди его сотрудников. Вакансия находилась в специализированном Telegram-канале. Обещали полный рабочий день в офисе и порядка 47 тыс. гривен (~100 тыс. рублей) с еженедельными выплатами на должности чат-менеджера. Рекрутер сразу пояснила, что работа будет «против страны-агрессора» в новом направлении «ректорат», а обман россиян «абсолютно безопасен». Небольшой нюанс: трудоустройство неофициальное и решить вопрос с мобилизацией не помогут. Схема следующая: из слитой базы данных россиян, которых они называют «орки», выбирается жертва. Предпочтительно старшего возраста. Менеджмент организаций считается лакомым кусочком. В соцсетях человеку пишут с фейковой страницы его руководителя или знакомого, пугают «непредвиденными обстоятельствами и серьёзными последствиями». Угрожают потерей работы или денег, уголовным делом, тюрьмой. На это уходит минут 15», - пишут про рекрутинг в колл-центры СМИ[35].

“С точки зрения криминалистики фиксируется трансграничный способ совершения IT-преступлений Доступность современных технологий, Интернет звонков позволяет совершать их из любой точки мира гражданам, находящимся в различных странах, возможности безналичных

35 https://russian.rt.com/ussr/article/1333919-skamery-ukraina-kiev-razvod-rektorat

расчетов привели к тому, что организаторы колл - центров находятся на территории одной страны, сам колл-центр на территории другой страны, а потерпевшие от действий злоумышленников - в третьей стране.

Например, на территории Российской Федерации пресечена деятельность колл-центра, по которому потерпевшими являлись иностранные граждане. Буквально в начале этого года совместно с белорусскими партнерами пресечена деятельность колл-центра, осуществляющего свою деятельность на территории Республики Беларусь, от действий которого пострадали более 100 тыс. российских граждан. При этом один из организаторов колл-центра также находился на территории Российской Федерации.

Масса источников подтверждает трансграничность преступности и причастность иностранных государств к организации преступлений на территории Российской Федерации.

Таким образом с учетом трансграничности на территории нашей страны действует низшее звено, которое, использует уязвимости современных технологий (банковские карт, оформленные на подставных лиц, сим-карты, оформленные на несуществующих лиц, анонимность при использовании мессенджеров). И в это низшее звено попадает молодое поколение.

Кроме того, основная масса похищенных денежных средств (сумма которых составляет 156 млрд рублей), с использованием услуг дропов и возможности бесконтрольного приобретения и продажи криптовалюты выбывает из юрисдикции Российской Федерации», - полагает генерал-майор МВД России Данил Филиппов.

Притом, в ходе расследования уголовных дел в отношении преступлений, предусмотренных ст. ст. 167, 205 УК РФ, установлено, что в их совершение вовлекаются «биодроны» из категории как пожилых граждан, так и подростков.

I.3. Целевые аудитории дистанционных преступлений

Как уже указывалось ранее, в настоящее время злоумышленники попытались втянуть в дистанционные преступления большую часть населения России и пострадавшие от этого наблюдаются в возрастных группах от 7 до 95 лет. Пострадали и почти все социальные группы, включая даже такую малочисленную как «депутаты Госдумы». Тем не менее, ряд возрастных категорий и социальных групп выглядят особенно уязвимыми.

В первую очередь, речь идет о детях и подростках. Как только несовершеннолетний приобретает навыки письма и получает доступ к мобильному устройству с интернетом, он попадает в зону риска.

В случае **детей** мошенники используют несколько подходов. В первую очередь, они используют уязвимость популярной игровой онлайн-платформы Roblox — ее «валюту». Нередко прямо в процесс онлайн-игр они предлагают детям пополнить ее запасы различными путями.

Это происходит, например так: «Пятиклассницу развели на 78 тысяч рублей от имени Королевы Роблокса. «Менеджер» Королевы пообещал девочке виртуальные монеты. Ночью с 9 на 10 августа 10-летней Даше (имя изменено) из г. Москвы в «Телеграме» позвонил неизвестный. Мужчина явно знал, что Даша любит играть в Roblox, и представился менеджером любимой блогерши девочки Королевы Роблокса (i.roblox.queen), на которую в YouTube подписаны 8 млн человек. «Менеджер» рассказал Даше, что может подарить ей виртуальную валюту, но для этого потребуется телефон её мамы. Девочка тайком взяла гаджет, созвонилась с «менеджером» по видеосвязи и по его инструкциям перевела нужную сумму на счёт некоей Елены Сергеевны. Сразу после разговора собеседник резко бросил трубку, а Даша испугалась и удалила все входящие звонки со смартфона. Впрочем,

скрыть пропажу денег от матери не удалось — днём того же дня мама школьницы написала заявление в полицию». Или так: «11-летняя девочка нашла в одном из мессенджеров якобы сверстницу, которая предлагала купить персонажей для компьютерной игры. Девочка по указанию неизвестного отправила мошенникам номер банковской карты мамы, а затем продиктовала коды из смс. Впоследствии выяснилось, что с карты были совершены покупки на сумму более 400 тыс. рублей»[36]; «9-летняя школьница из г. Казани перевела мошенникам 400.000 рублей с маминой карты, пытаясь купить игровую валюту для Roblox. Аферисты связались с девочкой через Telegram и обманом убедили её осуществить перевод денег через онлайн-банкинг матери»[37].

Впрочем, существуют и более простые схемы: «Мошенник уговорил 9-летнюю девочку из г. Москвы перевести 780 тысяч рублей со счёта родителей. Он сказал, что по ошибке отправил им миллион. Вечером 16 декабря у 9-летней Маши (имя изменено) зазвонил телефон, а конкретно — «Телеграм». Девочка подняла трубку и услышала голос неизвестного мужчины. Извиняясь, он объяснил, что по ошибке перевёл родителям Маши миллион рублей, и девочка должна помочь их вернуть. Маша согласилась помочь неаккуратному дяде, взяла телефоны родителей, зашла в банковские приложения (да, она знала пароли) и «вернула» мужчине 780 тысяч рублей. Когда родители вернулись, девочка поспешила их обрадовать и рассказала, что сделала доброе дело. Следователи квалифицировали это доброе дело как мошенничество»[38].

---

36 https://epp.genproc.gov.ru/web/proc_77/activity/legal-education/fraud?item=100132294

37 https://ayaznal.ru/riddles/moshenniki_iz_roblox_zaskamili_9_letnjuju_shkolnicu_na_400_000/2025-02-24-2422

38 https://www.gazeta.ru/social/news/2025/02/01/24975908.shtml

Контакты детей злоумышленники обычно узнают в чатах, куда внедряются под видом их сверстников. «Число мошеннических атак на детей в феврале 2025 года выросло в 5 раз по сравнению с декабрем 2024 года. По итогам месяца специалисты компании F6 зафиксировали около 600 случаев, когда аферисты «управляли» детьми, чтобы завладеть деньгами на счетах родителей. Чаще всего мошенники знакомятся с детьми в игровых чатах. Они могут попросить ребенка приложить палец спящего родителя к экрану смартфона или заранее подсмотреть пароли взрослых для входа в онлайн-банк, а затем войти в личный кабинет на устройстве и выполнить перевод. Также ребенка могут заставить взять телефон мамы или папы, сфотографировать экран с смс-кодом, а после удалить сообщение», - утверждают профильные специалисты[39].

Не менее уязвима возрастная категория **подростков**. Так же, как и дети, они могут потратить все родительские деньги на игровую валюту из сомнительного источника или вернуть несуществующий долг, однако при этом они равно уязвимы и перед «взрослыми» схемами. Например: «Вчера 15-летняя девочка передала более 320 тыс. рублей родительских сбережений курьеру. Ребенку позвонили мошенники и, представляясь сотрудниками сотовой компании, под предлогом продления договора заполучили код из смс. Затем по указанию лжесотрудника финмониторинга девочка, снимая свои действия на камеру мобильного телефона, взяла деньги, отложенные на ее обучение, упаковала их в коробку, перемотала скотчем, положила в рюкзак и передала прибывшему курьеру якобы для внесения их на безопасный счет. При этом злоумышленники запретили девочке кому-либо рассказывать о своих действиях. Вернувшаяся домой мама увидела беспорядок, расспросила дочь о случившемся, после чего обратилась к правоохранителям».

39 https://www.f6.ru/media-center/press-releases/scammers-attack-children/

Главная же опасность в случае подростков заключается в дистанционном вовлечении их в противоправную деятельность. Им предлагают стать дропперами и закладчиками наркотиков, а в наихудших случаях осуществить преступления диверсионного и террористического характера — поджечь релейные шкафы на железных дорогах, автотранспорт, локомотивы и даже вертолеты. Нередко отмечаются схемы, в которых целью преступников может быть одновременно финансовая выгода и совершение жертвой преступления. Как в этом случае: «Подростка, которого мошенники уговорили поджечь ТЦ в Нахабино, развели через бот для знакомств «Дайвинчик». Пацан просто хотел погулять с девочкой, но наткнулся на сложную схему.

По данным источников, 2 апреля 13-летний Роман (имя изменено) нашёл группу для знакомств «Дайвинчик», а там познакомился с некой 12-летней Марьяной. Девочка согласилась погулять, но сначала попросила Рому прислать свою геолокацию — мол, чтобы понять, где он живёт. Рома выслал геоточку, но Марьяна больше не отвечала — вместо этого неизвестный контакт прислал ему видеозапись, на которой мужчина с флагом Украины на рукаве обещал ударить ракетой по координатам Ромы.

Чат быстро удалили, после чего подростку написал другой неизвестный. Мужчина представился сотрудником ФСБ и сообщил Роме, что парень теперь изменник Родины, — потому что общался с украинским военным. За это Рому, а также его родителей скоро отправят в тюрьму. Пока пацан пытался прийти в себя, ему написал ещё один контакт. Некто представившийся сотрудником налоговой службы обещал прекратить уголовное дело за госизмену за 500 тысяч рублей.

Таких денег у Ромы, конечно, не было. Тогда семикласснику приказали поджечь машину и здание. Парню прислали 1000 рублей — на канистру бензина и зажигалку, — после чего он поджёг «Киа Соренто», припаркованный

на Школьной улице, а затем пошёл в ТЦ «Элизиум», где разлил бензин на полу магазина «Смешные цены» и устроил поджог»[40].

С другой стороны возрастной шкалы от действий преступников сильнее всего страдают **пенсионеры**, особенно в возрасте от 70 лет. Многие из них отличаются повышенной доверчивостью из-за возрастных изменений психики, кроме того значительная часть пожилых людей плохо разбирается в современных технологиях и слабо представляет последствия ряда своих решений.

К особому сожалению злоумышленники научились использовать против таких людей их положительную черту — патриотизм и доверие к отечественным правоохранительным органам, особенно спецслужбам. Из-за этой особенности именно пенсионеры чаще всего выступают в роли биодронов, атакуя военкоматы и отделения банков. Дополнительной уязвимостью военных пенсионеров, пенсионеров правоохранительной системы и любых иных пенсионеров, имевших доступ к гостайне (а также их супругов), является страх перед «особистами», а также хорошо известное мошенникам свойство испытывать доверие к говорящим командным тоном людям. Исходя из этого в их отношении часто работают бывшие или действующие сотрудники аналогичных украинских организаций.

Вот классический случай: «Мошенники обманули 81-летнюю пенсионерку из г. Москвы на 35 миллионов. Женщину даже убедили продать жильё, и теперь ей приходится снимать свою собственную квартиру, расплачиваясь за нее мебелью и техникой. В сентябре 2023 года Ларисе Викторовне (вдове генерала) поступило несколько звонков. Звонили якобы из ГУВД района и Сбербанка. Её предупредили, что сбережения в опасности и все деньги нужно перевести в

40 https://t.me/bazabazon/36563

другой банк. Поблизости как раз закрылись два Сбербанка. Для пущей убедительности ей позвонили по видеосвязи — она увидела перед собой Владимира Новикова в форме полковника и стала ему доверять. Он сказал, что помнит её мужа, который тоже когда-то работал в ГУВД. Позже к Новикову присоединился якобы сотрудник ЦБ РФ Андрей Карпов. Прислал свои документы, интеллигентно разговаривал. Лариса Викторовна сняла накопленные три миллиона и отдала курьеру, который пришёл от ЦБ. Звонки продолжились, аферисты сказали, что квартира пенсионерки в опасности и лучше продать её, пока это не сделали мошенники. По словам Ларисы Виктороны, на неё сильно давили и сомнений практически не было. Вскоре к ней пришли риелторы и покупатель, представившийся московским хирургом. Она продала ему квартиру за 29 миллионов рублей, ещё миллион заняла у подруги — он нужен был, чтобы быстрее решился суд по возврату квартиры. Мошенники обещали, что все деньги пенсионерка вот-вот получит обратно. Только в марте женщина решилась пойти в полицию и прокуратуру. Лариса Викторовна осталась одна с сыном-инвалидом без денег и жилья. Всю зиму она продавала мебель из квартиры, чтобы платить аренду новому хозяину её квартиры. Сегодня Ларису Викторовну заставили выехать из квартиры»[41].

Выделяя наиболее уязвимые социальные группы, также следует отметить **статусных и публичных людей**. «Статьи об известных людях в онлайн-энциклопедиях используются для выбора и подготовки атак на высокостатусных жертв. Преступники целенаправленно изучают биографии ученых, профессоров и авторов значительных научных открытий, чьи достижения подробно описаны. Мотивация злоумышленников основана на предположении, что такие личности обладают значительными финансовыми

41 https://www.ntv.ru/novosti/2823820/

ресурсами, а их профессиональная занятость и привычка к уважительному отношению ослабят бдительность. Подготовка к таким атакам ведется более тщательно. Часто используются варианты схемы «фейк-босс» с участием соответствующих по статусу звонящих. Так, в ходе одной из неудавшихся попыток мошенники использовали дипфейк мэра крупного города, где проживает заслуженный научный работник и преподаватель. Такого рода атаки удаются злоумышленникам не часто, но всегда характеризуются весьма существенным[42] ущербом или даже более трагическими[43] последствиями», - справедливо указывают СМИ[44].

Среди пострадавших из этой группы можно отметить депутата Дмитрия Певцова, певиц Ларису Долину и Хелависку, дочь пресс-секретаря Президента России Елизавету Пескову, профессоров Высшей школы экономики и докторов экономических наук Якова Уринсона (бывший министр экономики России) и Марка Урнова, политика Ирину Хакамаду, судью Наталью Ларину, балетмейстера Олега Виноградова, телеведущего Эдварда Радзинского, бывшего начальника Приволжской железной дороги Александра Храпатого, бывшего командующего сухопутными войсками генерала армии в отставке Николая Кормильцева. Есть в этом списке не только десятки профессоров, но и как минимум один академик РАН.

Особенно неприятно видеть среди пострадавших экс-начальника ФСБ по Москве и Московской области генерал-полковника Александра Царенко (потерял 1,5 млн.),

42 https://aif.ru/society/izobretatel-iz-peterburga-otdal-moshennikam-43-mln-rubley

43 https://aif.ru/incidents/mash-eks-professor-mgu-nayden-mertvym-posle-obshcheniya-s-aferistami-s-ukrainy

44 https://temryuk.ru/presscenter/news/slozhnye-mnogoetapnye-moshennicheskie-skhemy-vsegda-nachinayutsya-s-podgotovki/

бывшего начальника управления авиации ФСБ, Героя России, генерал-лейтенанта Николая Гаврилова (потерял 1,5 млн.), бывшего московского прокурора и специалиста по борьбе с аферистами Евгения Манеркина (потерял 20 млн.), директора административного департамента Минфина РФ Владимира Штопу (потерял 4 млн.) и советника генерального директора по образовательным проектам «Лаборатории Касперского» (специализирующейся на борьбе с киберпреступлениями) Вениамина Гинодмана (потерял 10 млн.).

В случае покушения на большие суммы злоумышленники работают целыми бригадами и активно применяют новейшие технологии. Так, преступная схема в отношении известной певицы Ларисы Долиной началась со сгенерированного нейросетью звонка якобы от имени ректора Московского государственного института культуры, где она возглавляет кафедру эстрадно-джазового искусства. Псевдоректор предупредила о звонке представителя «службы безопасности» института, который оперативно связал пострадавшую с «сотрудниками» ФСБ и Росфинмониторинга.

В настоящее все чаще используются дипфейки при видеосвязи. Как минимум в случае из городов Москвы и Санкт-Петербурга статусным людям регулярно поступают предложения выйти на видеоконференцию с главами этих городов. Получившие такой сомнительный опыт люди свидетельствуют о высоком качестве подделок — лжеСобянин и лжеБеглов сидят в узнаваемых кабинетах, правильно ведут беседу и делятся малоизвестными деталями из жизни предполагаемой жертвы. Суть беседы обычно сводится к тому, что ФСБ проявляет повышенный интерес к бизнесу уважаемого партнера, поэтому ценящий его вклад в градоустройство градоначальник готов оказать поддержку, предложив, например, контакт «своего человека в Конторе». Который и решит все проблемы через вывод денег на «безопасный счет» и прочие хорошо известные схемы.

«Аферисты стали рассылать приглашения на «личную видеоконференцию» с губернатором Петербурга Александром Бегловым. О новой схеме мошенничества предупредила пресс-служба Смольного. - Ни я, ни члены правительства, ни сотрудники моего аппарата на личную видеобеседу никого не приглашаем. Подобные сообщения - фальшивка, направленная на подрыв доверия к органам власти, - заявил Беглов», - писали об этом случае СМИ[45].

Публичным персонам также часто предлагается схема «лжеВикипедия». В ее случае поступает звонок от имени редакторов этой сетевой энциклопедии, которые зачитывают предполагаемой жертве посвященную ей статью, а затем предлагают получить доступ к ее редактированию через специальную программу, которую нужно скачать на телефон.

«Мошенники обманули писателя Эдварда Радзинского на 45 млн рублей. Злоумышленники позвонили Радзинскому после его творческого вечера 9 июля и представились сотрудниками «Википедии». Лжесотрудники онлайн-энциклопедии предложили обновить о нем информацию на сайте, но писатель бросил трубку. Тогда Радзинскому позвонили якобы из ФСБ, заявив, что мошенники хотят украсть и перевести ВСУ накопленные на квартиру деньги Радзинского. Писатель забрал избанка накопления в размере 45миллионов рублей и передал их «доверенному сотруднику Федеральной службы охраны». Курьера, 19-летнего студента, после задержали полицейские.[46] В июне аналогичным образом мошенники обманули художника Никаса Сафронова — сперва они представились сотрудниками «Википедии», а после взломали его «Госуслуги», аккаунт в WhatsApp и от имени Никаса стали просить других знаменитостей скинуть деньги на их счет».

45 https://www.spb.kp.ru/online/news/6288050/

46 https://www.gazeta.ru/culture/news/2024/07/22/23510635.shtml

С началом Специальной военной операции сформировалась новая социальная группа — **родные и близкие участников СВО**. Она также отличается особой уязвимостью к дистанционным преступлениям. Нередко потенциальной жертве здесь угрожают смертью родных и близких (особенно уязвимы здесь родственники пропавших без вести или попавших в плен военнослужащих), спасти которых может только теракт. «Жена российского военного, который находится в плену у ВСУ, получила видео с пытками супруга и требованием совершить теракт, чтобы они прекратились. Кадры РИА Новости предоставил источник. На них неизвестный избивает дубинкой российского пленного, который представился как "рядовой Полий»[47].

Известны и другие методы воздействия на эту целевую аудиторию. «Мошенники стали обманывать участников СВО и их родственников. Злоумышленники пользуются малой информированностью и невысокой финансовой грамотностью участников СВО, а также сложной морально-психологической жизненной ситуацией родственников, у которых отсутствует прямая связь с военнослужащим. Известную многим схему мошенников с безопасным банковским счетом стали применять на участников СВО, но со своими нюансами.

Так, стали известны случаи, когда с военнослужащим связываются злоумышленники и сообщают им, что в связи с наложением на военнослужащего дисциплинарного взыскания, с его выплат будут производиться удержания денежных средств. Для большей убедительности мошенники могут прислать поддельную выписку из приказа Департамента финансового обеспечения Минобороны России. После этого, военнослужащему предлагается перевести свои денежные средства на безопасный счет, который подконтролен

47 https://ria.ru/20241002/plennyy-1975999405.html

мошенникам, таким образом участники СВО теряют свои денежные средства.

Другим способом мошенники организуют в социальных сетях фейковые группы поиска пропавшего военнослужащего или находят реальные группы, где состоят родственники участников СВО. Мошенники предлагают за денежное вознаграждение предоставить родственникам информацию о местонахождении и состоянии здоровья участников СВО, в результате чего родственники теряют денежные средства.

Еще одним циничным способом мошенники действуют в отношении вдов и матерей, которым сложно отфильтровать звонки и сообщения от настоящих заботящихся о них представителей власти. Так, притворяясь ими, мошенники осуществляют телефонные звонки родственникам, в ходе которых сообщают о захвате в плен, ранении или даже смерти близкого им человека. После чего, для того что бы предоставить родственникам полную и достоверную информацию, организовать транспортировку или лечение, просят у них денежные средства с целью их фактического хищения.

Например, родственница участника СВО проживающая г. Пятигорск, попавшего в плен, перевела мошенникам 250 тыс. рублей за непривлечение её сына украинской стороной к уголовной ответственности. В Ростовской области женщина «организовывала поиски пропавших военнослужащих», фактически просто похищая денежные средства, застав родственников врасплох. На неё возбуждено уголовное дело»[48].

Именно на эту группу ФОИВам следует обратить особое внимание при проведении профилактической работы.

Очень уязвимой к дистанционным преступлениям оказалась социальная группа **школьных педагогов**, которые

48 https://gurb.mosreg.ru/sobytiya/novosti-ministerstva/kakie-sxemy-ispolzuyut-mosenniki-v-otnosenii-ucastnikov-svo-i-ix-rodstvennikov

помимо классических схем мошенничества страдают еще и от украинских пранков (т.е. провокаций с целью подрыва доверия к российской власти, в ходе которых в школы получают письма от якобы вышестоящих инстанций). «Российские учителя изготовили шапочки из фольги в рамках патриотической акции. Это был пранк Владислава Бохана. Акционист вновь разослал по школам центральной России требование от имени «Единой России» провести патриотическую акцию. На этот раз необходимо было изготовить из фольги «Шлем отечества» для демонстрации готовности к защите от облучения спутниками НАТО. На требование откликнулись 7 школ: МКОУ Бобровский образовательный центр «Лидер», Крикшанская СШ №3, Колодезянская СОШ, Нововоронежская СОШ №1, Архангельская СОШ, а также Байчуровская и Никольская СОШ. Две последних привлекли к изготовлению шапочек детей, а педагог одной из них потребовала диплом за участие в акции. Бохан пояснил, что продолжает исследование фашизации России в рамках выявления признаков «вечного фашизма» согласно трактату Умберто ЭКО. «Шапочки» проиллюстрировали веру населения России в теорию заговора, тогда как предыдущее аналогичное поручение учителям – проведение бессмысленной акции «Русский бег» (без уточнения, куда и зачем) – готовность совершать действие ради действия. Напомним, ранее Бохан в рамках сходных акций убедил российских учителей составлять списки для отправки школьников на перевоспитание в лагеря, молиться на иконы Бандеры и Тихановской, проводить патриотическую акцию под слоганом «Один народ, одна нация, один праVитель» в рамках программы «Единой России» «Труд освобождает» и т. д. Свои акции Бохан называет исследованием проявлений фашизма в современной России: безоговорочного подчинения начальству, действием ради действия и других его признаков», - вот так эти действия трактуют враждебные России СМИ.

Особый вид дистанционных преступлений практикуется в отношении **российского духовенства,** в первую очередь самого многочисленного — православного. Приведем выдержку из посвященного этой проблеме статьи: «Примерно в 2016-17 гг. сотни российских архиереев, наместников монастырей, благочинных и даже настоятелей соборов получили звонки от имени якобы архиепископа Петропавловского и Камчатского Артемия, которой просил оплатить билет до Москвы «очень набожному и трудолюбивому» иеромонаху, у которого якобы заболела мать. В случае звонков в женские монастыри иеромонах менялся на не менее набожную и трудолюбивую монахиню. В итоге десятки людей лишились от 30 до 50 тысяч, что по нынешним меркам убытки совершенно смехотворные.

Так, совсем недавно из-за мошеннических схем Марфо-Мариинская обитель потеряла 26 млн. руб, московский протоиерей Анатолий Нагорный — 17 млн., а Выксунская епархия — 2,7 млн. Вот типичные новости наших дней: «Митрополит Екатеринбургский и Верхотурский Евгений предупредил: если Вам поступают звонки от имени митрополита с неизвестного номера и просят о денежной помощи – на создание фильма или на приезд съёмочной группы – лучше сразу положите трубку»[49], «Сегодня нескольким сотрудникам Челябинской епархии в телеграме поступили сообщения от священнослужителей епархии. В них «батюшки» объясняли, что сейчас в управлении проходят проверки и нужно честно ответить на вопросы инспектора по безопасности Юрия Михайловича Дубровина».[50] Братскую епархию затерроризировал псевдоСилуан (епископ Петергофский), а соавтору этой статьи писали от имени племянника Святейшего Патриарха.

---

49 https://ural-meridian.ru/news/411346/

50 https://mitropolia74.ru/novosti/telefonnye_moshenniki_ispolzuyut_imena_s...

Впрочем, чаще всего звонки и сообщения поступают от имени управляющего делами Церкви митрополита Воскресенского Григория и личного секретаря Святейшего Патриарха епископа Раменского Алексия. Священнослужителей могут поздравить с реально состоявшимся новым назначением или же сообщить о назначении вымышленном, а затем намекнуть на благодарность, которая обычно составляет порядка полумиллиона рублей «на новые облачения/панагии Патриарху». Мирянам обычно сообщают о высоком ордене, который тоже небесплатный и дорогой.

Приведем слова игумена Кирилла (Сахарова), который сам стал жертвой мошенников и поведал о своем опыте в специальном материале. «Вдруг раздается звонок: помощник сообщает, что меня просит срочно позвонить епископ Алексий. «Говорил с кавказским акцентом. Представился секретарем Патриарха», — добавила она. Судорожно соображаю, кто бы это мог быть. В Москве я знаю только одного епископа Алексия – наместника Свято-Данилова монастыря. Он, однако, не является секретарем Патриарха. Может быть, меня вспомнил грузинский Патриарх, с которым я общался в Тбилиси много лет назад? Не дозвонился. Чтобы лишний раз не мешать участникам конференции, попросил помощника, чтобы «епископ Алексий» сам мне позвонил. Раздался звонок, на экране возникла фотография архиерея. Спрашиваю звонившего: «Простите, я что-то не припомню в Москве епископа Алексия» — «Меня недавно рукоположили» — «Да, да» — вспомнил я, что было решение Синода о рукоположении архимандрита Алексия (Турикова), секретаря Патриарха во епископы. «Епископ Алексий»: «Отец Кирилл, Вы родились 22 октября 1957 года?» — «Да» — «Вы закончили истфак МГПИ, Московскую Духовную семинарию, Московскую Духовную академию, аспирантуру при ОВЦС?» Я все подтверждаю. «Вас срочно вызывает Святейший – он хочет Вас назначить

наместником Троице-Сергиевой Лавры». Ошалев от такой информации, я перестаю что-то соображать»[51]. В этой истории все кончилось относительно хорошо — отец Кирилл потерял время и душевное равновесие, однако сохранил деньги»[52].

Также следует включить в зону особого риска **жителей прифронтовых территорий**. Они особенно активно атакуются как мошенниками, так и подстрекателями к терактам и диверсиям.

Глава II. Виды дистанционных преступлений.

II.1. Дистанционные хищения средств

Как уже упоминалось в предыдущих разделах, миллионы граждан России пострадали от дистанционных преступлений, в первую очередь дистанционного мошенничества. Урон от него можно условно разделить на четыре уровня:

- Низкий — тысячи-сотни тысяч рублей.
- Средний — миллионы рублей.
- Высокий - потеря всех средств, недвижимости и закредитованность.
- Экстремальный — вовлечение в диверсионную или террористическую деятельность после одного из трех вышеперечисленных вариантов.

Известны десятки схем мошенничества, в рамках которых можно потерять от тысяч до сотен миллионов рублей. Фейковые билеты в театры и концерты, обман на маркетплейсах, предложения «поддержать дочку в конкурсе»

51 https://ruskline.ru/news_rl/2024/04/20/kak_menya_razveli_na_namestnika_t...

52 https://radonezh.ru/2024/09/06/roman-silantev-vas-bespokoit-upravlyayushchiy-delami-ili-kak-ne-stat-zhertvoy-ukrainskih

или «в долг оплатить покупку» через взломанные аккаунты в мессенджерах наносят гражданам России относительно небольшой урон, однако есть и более опасные варианты.

Преступники применяют для обмана граждан **два подхода**.

В первом подходе они пытаются вовлечь в свои схемы случайных людей, которые выявляются массовыми обзвонами или рассылками. Для этого используются украденные базы данных, в которых как минимум содержатся фамилия, имя и отчество потенциальной жертвы. Здесь можно выделить 20 самых распространенных вариантов.

1. Продление договора с оператором мобильной связи.

«Если вам звонят от имени мобильного оператора, чтобы продлить действие симкарты, — скорее всего, это мошенники. Звонящий утверждает, что вот буквально завтра заканчивается ваш контракт на мобильную связь. Если его не продлить, вы не сможете звонить, отправлять смс и пользоваться мобильным интернетом. Номер у вас отберут и передадут другому человеку. Мошенник предлагает продлить договор без посещению офиса. Достаточно продиктовать код из смс. Конечно, коды из смс никогда и никому говорить нельзя, и многие это знают. Если отказаться, мошенник не будет упорствовать и повесит трубку: его ждет следующий из списка обзвона. Но если почувствует ваши сомнения, постарается дожать: мол, речь о деньгах не идет и вы ничем не рискуете. Вам же хотят сэкономить время. Этот код нужен мошенникам, чтобы получить доступ в личный кабинет жертвы на сайте оператора. Там преступники устанавливают переадресацию звонков сообщений на свой номер. Так они будут узнавать все секретные коды, в том числе от банков. В результате аферисты смогут получить доступ к банковским кабинетам, снять деньги со счетов и даже попытаться оформить кредиты».

2. Продление договора связи стационарного телефона

«В разных[53] регионах России фиксируются мошеннические звонки на домашние телефоны. Злоумышленники представляются сотрудником Ростелекома и под предлогом «продления договора связи», просят сообщить код авторизации, пришедший в SMS на мобильный телефон жертвы. Получив код, злоумышленники получают доступ к важным аккаунтам, позднее следует новый звонок — уже от имени правоохранительных органов или Росфинмониторинга. Аферисты заявляют, что с аккаунтом жертвы или ее счетами «проводятся незаконные операции», и под видом «защиты» или «проверки» требуют передать деньги курьеру. Именно таким образом пенсионер из Нижнего Новгорода лишился 4,5 млн рублей».

3. «Медицинские схемы»

Это один из самых распространенных и опасных для пенсионеров вариантов. В его случае жертву могут «записать на флюорографию», попросив продиктовать номер медицинского полиса или СНИЛСа, попросить помочь в обновлении данных для базы медучреждения, предупредить о необходимости смены медицинского полиса. Например: «Прокуратура предупреждает о новой схеме мошенничества

Новая схема мошенничества[54]: телефонные аферисты начали представляться якобы сотрудниками единой медицинской системы и под предлогом изменения данных о пациенте в системе уговаривают установить программы и похищают денежные средства. Так, жителю района Свиблово в мессенджере поступил звонок от неизвестной женщины,

53 https://regions.ru/serpuhov/bezopasnost/novaya-shema-obmana-aferisty-pod-vidom-rostelekoma-kradut-akkaunty-na-gosuslugah

54 https://epp.genproc.gov.ru/web/proc_77/mass-media/news?item=97176583

которая представилась медицинским работником и сообщила, что в его медицинской карте устаревшие данные. Чтобы их обновить нужно четко следовать ее инструкциям. Спустя несколько минут мужчине поступило смс-сообщение, якобы содержащее инструкцию по обновлению. Пенсионер открыл файл, установил на свой телефон приложение, после чего экран телефона потемнел, а звонившая аферистка попросила не трогать его некоторое время, т.к. идет обновление. Когда «перезагрузка» завершилась, пострадавший обнаружил, что через онлайн приложение неизвестные перевели с его карты более 1,3 млн рублей.

«Пришла я к клиентке (женщина 83 года). После оказания услуги, стали мы с ней пить чай, и вот она мне рассказывает, что недавно ей звонили мошенники. Сперва позвонили якобы из поликлиники и пригласили на ЭКГ, но для записи «потеряли» полис и нужно его найти в базе. Выманили у нее паспортные данные и СНИЛС. Тут внезапно звонок обрывается со словами в трубке «вам звонят мошенники, звонок будет прерван». О такой схеме я уже слышала. Но бабушка нет, она впервые на такое нарвалась. Побежала она в банк, наложила запрет на банковские операции. Напилась таблеток от давления. И вот сидим мы, пьём чай. Тут при мне звонок по Ватсаппу. Я сразу понимаю, что мошенники решили бабушку добить, но прерывать их не стала, хотела посмотреть, что в итоге они будут от нее требовать. Хотя, знак ей подала, что это мошенники и что бы она не сильно откровенничала с ними. На аватарке герб, а преставился молодой человек кем-то из Роспотребнадзора. Хотя, в Ватсаппе звонок был подписан входящий как «Лизонька». И вот, они начали разводить ее на смену пароля от ГосУслуг. Якобы мошенники пытались изменить пароль и телефон привязанный к Госуслугам. Минут 30 обхаживали. Спросили даже как зовут её собачку, какой она породы и какого цвета. А бабушка и рада вниманию, отвечает на все их вопросы. И тут просит этот «Лизонька»

из Роспортребнадзора записать их разговор через диктофон, чтобы все якобы было официально, и будем менять привязанный телефон к Госуслугам. А так как у бабушки нет диктофона, он говорит ей нажать три точки внизу экрана, которые видны при разговоре по Ватсаппу. А в трёх точках кнопка «Демонстрация экрана». Это якобы запись разговора, с его слов. И бабушка тянется пальцем нажать! Даже я на долю секунды задумалась, что это может быть действительно запись разговора. Но там четко и ясно написано «демонстрировать экран». Тут я уже понимаю, что нужно вмешаться и кричу в телефон, чтобы шли вон! Бабушка испугалась, попыталась закрыть микрофон рукой и шепчет мне: «ты что, это же не мошенники, а правда Роспортребнадзор!» В этот момент я понимаю, как же легко развести стариков. Если бы она нажала эту кнопку, то мошенникам полностью бы предоставила доступ к своему экрану, и тут бы посыпались у нее смс со всякими кодами доступа. Она бы даже сообразить ничего не успела. Отобрала у нее силой телефон, послала «Лизоньку». Сказала бабушке сходить в МФЦ написать заявление о запрете кредитования. Чтобы уж точно никто без нее никакие кредиты на нее не навешал. Пока больше ей не звонили».

«Мошенники убедили студентку из Владивостока прислать им интимное видео для проверки тела на отсутствие взрывных устройств. А также сдать семейные драгоценности в ломбард и перевести 230 тысяч рублей. Вечером 12 марта студентке ВГМУ Анастасии (имя изменено) позвонили якобы из поликлиники: для уточнения данных её попросил продиктовать коды из присланных смс вместе с паспортными данными. 18-летняя девушка назвала цифры и почти уже забыла о звонке, как пришла тревожная новость: «сотрудником поликлиники» оказался мошенник, и он уже якобы взломал аккаунт студентки в «Госуслугах». По указанному в сообщении номеру Анастасия обратилась в лжетехподдержку «Госуслуг», где ей посоветовали скорее

перевести все сбережения на безопасный счёт. Студентка так и поступила: сначала перевела 105 тысяч рублей, затем — ещё 125, вырученные от сдачи драгоценностей родных в ломбард. Напоследок мошенники попросили Анастасию снять видео голышом — чтобы убедиться, что на её теле нет взрывных устройств. Девушку ничего не смутило: она сняла нюдс, затем отправила аферистам. Только после этого до студентки начало доходить, что её развели. Девушка удалила видео и пошла в полицию».

4. Замена кодов или ключей для домофона

«В Казани женщина перевела мошенникам почти 500 тыс. руб. после звонка о замене кодов домофона. Злоумышленники представились сотрудниками различных ведомств и убедили женщину перевести деньги на «безопасный счет». Об этом сообщает пресс-служба Управления МВД России по Казани. Днем пенсионерке позвонил неизвестный, представившийся сотрудником организации по смене кодов домофонов. Он попросил продиктовать временные коды, которые поступят на телефон женщины. Она назвала нужную комбинацию цифр. Затем с пенсионеркой связались люди, представившиеся сотрудниками Роскомнадзора и Росфинмониторинга. Они запугали женщину возможными несанкционированными переводами и убедили перевести полмиллиона руб. на «безопасный счет». Мошенники вызвали пострадавшей такси до ближайшего банкомата и запретили общаться с сотрудниками банка и родственниками. Вечером женщина рассказала о произошедшем дочери, которая объяснила, что мать стала жертвой мошенников».

5. Перерасчет пенсии или трудового стажа

«Потенциальная жертва получает в мессенджере звонок якобы от Социального фонда. Собеседнику предлагают записаться на «перерасчет пенсии» и просят код из СМС. Затем

поступает следующий звонок от аферистов. В этот раз они представляются службой поддержки портала и сообщают, что кто-то пытается украсть данные пользователя. Параллельно человек получает поддельные СМС о входе в личный кабинет в разных микрофинансовых организациях, якобы оповещения о переводе кредитных денег в разные банки. После этого с жертвой связывается «полиция» или «банк», для «защиты» средств они предлагают перевести накопления на «безопасный счет».

«Телефонные мошенники обманывают пенсионеров под предлогом перерасчета трудового стажа и похищают деньги, угрожая уголовным делом за оказания помощи Украине. Это следует из материалов МВД, с которыми ознакомился ТАСС.[55] Так, неизвестные звонят пожилым людям, представляются работниками Пенсионного фонда и просят продиктовать им паспортные данные якобы для перерасчета трудового стажа. На этом разговор заканчивается. Затем с потенциальной жертвой связывается псевдоправоохранитель, который сообщает о том, что по паспортным данным человека осуществлен денежный перевод на Украину, в связи с чем в отношении него возбуждено уголовное дело. Воспользовавшись взволнованным состоянием человека аферисты убеждают пенсионера снять сбережения и для избежания неприятностей и сохранности передать их курьеру. Что человек и делает, лишаясь своих накоплений».

6. Неправильно оформленный запрет на кредиты

«Мошенники воспользовались недавно заработавшим самозапретом на кредиты для обмана граждан, сообщили «Известиям» в Ассоциации развития финграмотности.[56] Они

55 https://www.kommersant.ru/doc/7622905

56 https://iz.ru/1852436/natala-ilina-evgenii-gracev-anna-kaledina/ne-dat-vzat-mosenniki-ispolzuut-samozapret-na-kredity-dla-obmana

звонят людям от имени сотрудников «Госуслуг» и уверяют, что запрет установлен неверно — чтобы исправить ситуацию, нужно пройти по ссылке, которую присылают в мессенджере, якобы чтобы исправить заявление. После того, как человек по ней переходит, он попадает на сайт, имитирующий «Госуслуги», вводит свои данные для входа, и они попадают к мошенникам».

7. Звонок от «дочери» или «сына» с применением дипфейков

Жительница Воронежа рассказала об удивительном способе обмана с помощью видео и голоса ее дочери. Об этом пишет kp.ru.[57] Мать студентки рассказала, что ей поступил видеозвонок от дочери. Она находилась в странном месте, за ее спиной было видно решетку, и женщина подумала, что девушка попала в отделение полиции. В ходе разговора «дочь» сказала, что у нее проблемы, и требовала без вопросов перевести 100 тысяч рублей.

— Все объясню тебе позже, когда ты переведешь. Я сейчас в полиции. Телефон будет отключен. Как только деньги переведешь, меня отпустят, и я сразу тебе позвоню, — рассказала о звонке мать. По ее словам, номер счета был отправлен ей в СМС по номеру телефона. Женщина отправилась к банкомату, чтобы пополнить счет, но тут уже позвонила настоящая дочь. Оказалось, что с ней все в порядке. Как выяснилось, мошенники подделали лицо девушки с помощью дипфейка и хотели развести ее мать на 100 т. р.

8. «Приглашение в коллегию присяжных» или «повестка в суд»

«Мошенники начали через электронную почту или мессенджеры вызывать россиян для якобы участия в коллегии

57 https://www.kp.ru/daily/27631.5/4981538/?utm_source=yxnews&utm_medium=desktop

присяжных заседателей, для отказа от которого требуют переходить по ссылкам и указать причины неявки, рассказал РИА Новости[58] руководитель центра правопорядка в Москве и Московской области, юрист Александр Хаминский. Как указал юрист, мошенники начали писать гражданам от имени сотрудников силовых структур и направлять якобы вызовы в правоохранительные или налоговые органы в связи с подозрением в соучастии в мнимом преступлении. Злоумышленники к таким «вызовам» зачастую прикрепляют активные ссылки, переход по которым предоставит мошенникам доступ к паролям от различных приложений, включая банковские. «Кроме того, могут приходить сообщения о том, что гражданин выбран для участия в коллегии присяжных заседателей. При этом за неявку обещают наступление административной и уголовной ответственности. Для того чтобы отказаться от этой обязанности, также предлагают нажать на ссылку в вызове для указания причин невозможности участия в коллегии присяжных», — предупредил Хаминский».

«У меня в суде сейчас находится дело о разводе с супругом (на определенный день и время назначена дата заседания). 4 октября мне звонит некий Чернов из суда, говорит, что он ведёт мое дело и есть возможность приехать в суд, написать заявление, тогда нас с мужем быстрее разведут, не нужно будет тратить 3 месяца на примирение, которое даётся в суде. Он называет полные данные мои, время и дату заседания (я на тот момент не знаю ещё, что вся эта информация в открытом доступе в интернете находится). Соответственно, я проникаюсь к нему полным доверием. Он говорит, что сейчас в судах усилена безопасность и поэтому, чтобы войти в суд, нужен специальный код, он мне его как раз сейчас вышлет и я должна буду ему его назвать.

58 https://ria.ru/20250104/moshennichestvo-1992454485.html

Мне приходит код с «Госуслуг», я называю ему код. После того, как положила трубку, я сразу поняла, что меня развели. Позвонила в полицию, собралась к ним ехать, по дороге мне позвонили из «Госуслуг», сказали, что мой профиль взломали, но сотрудники «Госуслуг» вовремя остановили мошенничество, профиль мой заморожен, но произошла утечка данных моих и теперь мошенники берут на меня кредиты.

Чтобы помочь мне сохранить свои сбережения, меня перевели на сотрудника Росфинмониторинга, который объяснил мне, что прямо в данный момент мошенники оформили на меня кредит на 300 тысяч руб. и Центробанк приостановил эту операцию. Дальше он соединил меня с сотрудником ФСБ. Всё очень грамотно было сделано, речь, специальные термины, в Телеграм у сотрудника ФСБ в имени стоял реальный номер фсбшников, только сам номер мобильный был скрыт, я это всё позже увидела и была уверена, что мне звонят прямо из ФСБ. Так как он сказал, что по инструкции их начальства я должна пройти на официальный сайт ФСБ и убедиться, что мне звонят не мошенники, в действительно сотрудник ФСБ.

Дальше мне было сказано, что деньги с кредита переводились на ВСУ, я прохожу по делу как обвиняемая. естественно, в этот момент, уровень моей тревожности повышается, а уровень рационального мышления уходит на второй план.

Мне говорят, что я должна четко действовать под руководством сотрудника Росфинмониторинга... Далее я беру кредит под его руководством (якобы это фиктивный кредит 380 тысяч руб., который даже не отобразится в БКИ), снимаю деньги, отправляю их на счёт, который он мне указал. Всё это мы делаем для того, чтобы поймать нечестного сотрудника банка, который якобы слил мои паспортные данные мошенникам. В общем, когда мне в «Почта-банке» одобрили ещё один кредит на 500 тысяч и я опять их должна была перевести, я задумалась... И всё поняла...».

9. «Квартира выставлена на продажу»

«В правоохранительные органы обратилась 77-летняя местная жительница, которая стала жертвой мошенников.[59] Пенсионерке в мессенджере позвонил якобы правоохранитель и сообщил, что ее квартира выставлена на продажу злоумышленниками. Чтобы не потерять недвижимость, женщине порекомендовали самостоятельно ее продать и перечислить вырученные деньги на «защищенный счет». При этом заверили, что жилище останется в ее собственности. Потерпевшая выполнила все рекомендации и за несколько платежей перевела мошенникам около 50 тысяч долларов. Лишь когда новая владелица попросила ее покинуть квартиру, а звонивший перестал выходить на связь, женщина поняла, что стала жертвой аферистов».

10. Замена электросчетчиков

«Мошенники выманивают код для доступа к «Госуслугам», представляясь сотрудниками крупных энергосбытовых компаний. Все больше пострадавших фиксируется от данной мошеннической схемы, которая распространилась по всей России: им поступают звонки от якобы представителей коммунальных служб. «Специалисты» назначают время для поверки и замены электросчетчиков, сообщают о необходимости перерасчета платежей или предлагают скидку на ЖКХ. «Каким бы ни был предлог, цель одна — запросить у жертвы код из SMS для доступа к «Госуслугам». Как сообщает[60] Прокуратура города Москвы, 71-летней пенсионерке позвонил неизвестный и сообщил о необходимости поверки счетчиков. Под этим предлогом

59 https://www.sb.by/articles/obmanutaya-moshennikami-minchanka-soglasilas-stat-ikh-kurerom-v-mvd-rasskazali-podrobnosti.html

60 https://epp.genproc.gov.ru/web/proc_77/mass-media/news?item=100706946

мужчина уговорил женщину продиктовать поступивший в смс код, с помощью которого был получен доступ к личному кабинету госуслуг. Затем в мессенджере пенсионерке пришло смс о том, что под залог ее квартиры оформлен кредит и номер телефона для обратной связи. Позвонив по телефону, женщина разговаривала уже с лжесотрудниками роскомнадзора и финмониторинга. Аферисты убедили ее открыть новый счет в банке, на который перевести сбережения, включив демонстрацию экрана. Затем злоумышленники сообщили пенсионерке, что банковская карта скомпрометирована и ее нужно передать курьеру, который выдаст ей новую карту. Передав криминальному курьеру банковскую карту, женщина обнаружила, что аферисты похитили с нее 2 млн рублей».

11. Декларирование денежных средства

«Как сообщает прокуратура города Москвы, все началось со звонка. 72-летней москвичке позвонила любезная девушка и сообщила, что необходимо прийти и получить доплату для Ветеранов труда. Девушка сказала, что будет много людей, а она может оформить все без очереди, для этого нужен только номер СНИЛС, который пенсионерка ей продиктовала.

Дальше в дело вступили «правоохранители», которые напугали женщину, сообщив, что она якобы перевела деньги недружественной стране и теперь находится на контроле. Окончательно запугав пенсионерку предстоящим визитом «сотрудников» с понятыми, лжеследователь сообщил, что все имеющиеся дома деньги необходимо «задекларировать» и передать «дежурному» по району, который придет к ней домой. После проверки информации все денежные средства обещали вернуть. Введенная в заблуждение пенсионерка передала женщине-курьеру более 1,3 млн рублей и 1 тыс. долларов США.

На следующий день к пенсионерке приехал курьер и передал ей коробку, в которой, со слов «следователя»,

находились деньги, а также два конверта с документами, однако вскрывать коробку пенсионерке запретили, убедив, что это возможно только в присутствии уполномоченного сотрудника и понятых.

Через два дня женщине вновь позвонили и начали убеждать в необходимости дальнейшей декларации денежных средств, находящихся на ее счетах в банке. Однако она заподозрила неладное и обратилась в правоохранительные органы».

12. Подарок с подвохом

«Недавно профильный Telegram-канал «Эксплойт» об интернет-технологиях опубликовал историю девушки-врача. Ей позвонили в дверь и передали анонимный подарок — букет цветов. Это — первый этап схемы. Получатель уверен, что это приятный сюрприз, и принимает подарок. Единственное, что его заботит, — это личность отправителя: кто же, мол, этот тайный поклонник? Через некоторое время начинается второй этап: злоумышленники звонят жертве и вежливо просят помочь. Они объясняют, что курьер не успел оформить какие-то документы или допустил ошибку, а им для строгой отчетности нужно знать, что букет точно дошел получателю. Есть и другая вариация второго этапа: злоумышленники звонят и говорят, что произошла ошибка, и подарок предназначался другому человеку.

Дальше схема начинает напоминать любые другие. Злоумышленники говорят нечто вроде: «Если вам доставили букет, и с ним всё хорошо, продиктуйте, пожалуйста, код из СМС-сообщения». Либо, если проигрывается сюжет «произошла ошибка», фраза звучит как: «Для отмены заказа продиктуйте код из СМС».

В некоторых случаях жертве через мобильный поступают деньги (обычно около 10-15 тыс.), а затем ее требуют их вернуть через СМС-код, запугивая уголовной ответственностью за кражу.

13. Имитация взлома Госуслуг

Мошенники используют схему обмана[61] со «взломом» профиля на «Госуслугах». Суть схемы: злоумышленники отправляют на почту человека письмо с предупреждением о входе в аккаунт с «нового устройства». Аферисты оставляют и номер сотрудника «техподдержки», который на самом деле перенаправляет жертву в украинский колл-центр. Похожая схема[62] с указанием фейкового номера поддержки также применяется на созданных мошенниками справочных сайтах.

14. Инсценировка похищения ребенка

«Угрожали тюрьмой и детским домом: телефонные мошенники инсценировали похищение ребенка и требовали 3 млн рублей у родителей в качестве выкупа.

Аферисты позвонили 11-летнему мальчику и, представляясь сотрудниками «Роскомнадзора», сообщили, что родители якобы являются пособниками преступников и необходимо выполнять телефонные указания, иначе родителей посадят в тюрьму, а его отдадут в детский дом. Испуганный ребенок, действуя по указанию злоумышленников, провел обыск в квартире, но ничего не нашел. Затем звонившие сказали мальчику сесть в такси и доехать якобы до их «сотрудницы», которую они выдавали за правоохранителя. У подъезда жилого дома по ул. Матроса Железняка ребенка встретила пожилая женщина, которая незадолго до случившегося сама стала жертвой мошенников и действовала по их указанию. Она проводила мальчика в к себе квартиру, где спустя непродолжительное время ребенка обнаружили уже настоящие правоохранители. Родители мальчика пояснили, что им звонили неизвестные, сообщали, что сын похищен

61 https://t.me/cyberpolice_rus/2771

62 https://ria.ru/20241223/moshenniki-1990761586.html?ysclid=m50ujw63cm44955532

и требовали выкуп 3 млн рублей, а также присылали фото ребенка. Мальчик передан родителями, его жизни и здоровью ничего не угрожает».

15. Лжедоставка

«Одна из новых схем получила название «Вам доставка». Злоумышленники эксплуатируют популярность интернет-торговли. Человеку поступает звонок якобы от службы доставки известного (а иногда и выдуманного) маркетплейса. Голос на другом конце провода сообщает радостную новость: долгожданная посылка оплачена отправителем и уже в пути. Для пущей убедительности имитируется рабочий шум офиса на фоне, а «сотрудник» обращается к жертве по имени-отчеству. Суть легенды сводится к тому, что нужно лишь сверить номер квитанции, который вот-вот придёт в SMS. И вот тут начинается самое главное: сообщение действительно приходит, но с подозрительной пометкой «код подтверждения». На осознание того, что это ловушка, у жертвы буквально одна секунда. Если не среагировать мгновенно, деньги уйдут моментально».

«Всё началось 20 февраля, когда Мише позвонили с незнакомого номера. Голос на том конце представился сотрудником службы доставки и с ходу ошарашил: мол, посылка на его имя вот-вот уйдёт на утилизацию, если он срочно не продиктует код из СМС. «Спаси заказ, парень!» — давили на жалость мошенники. Миша, не заподозрив подвоха, послушно зачитал цифры. Кто бы мог подумать, что этот код станет ключом к кошмару?»[63]. Кстати, в этом случае убытки составили 200 млн. рублей.

63 https://www.mk.ru/incident/2025/02/25/moskovskiy-shkolnik-otdal-moshennikam-200-millionov-rubley.html

16. Саморазоблачение мошеников

Мошенники усыпляют[64] бдительность россиян, имитируя по телефону свое разоблачение. Суть схемы: аферист звонит от имени курьера, неумело пытается выведать СМС-код, который тут же приходит с неизвестного номера. Через секунду он просит «повисеть» на линии и «прокалывается», якобы забывая выключить микрофон. «За кадром» он с подельниками обсуждает, как выведать тот самый код из СМС. В этот момент человек на другом конце провода все «понимает», но игра на этом не заканчивается. В нее вступает фейковый сотрудник «Роскомнадзора», который «засек» злоумышленника. Он звонит жертве, сообщает о мошенниках и просит уже ему — настоящему сотруднику — сообщить персональные данные или код из СМС.

17. Онлайн-обыск

«22 января было возбуждено очередное уголовное дело о мошенничестве, жертвой которого стала 18-летняя бердчанка. Схема началась традиционно: на телефон девушке пришло смс-сообщение с неизвестного номера о том, что кто-то получил доступ к её личному кабинету на Госуслугах. В этом же сообщении был указан телефон техподдержки, по которому взволнованная бердчанка тут же позвонила.

С этого момента девушка и попалась в лапы аферистов. Там ей сообщили, что её личный кабинет взломан и перевели на якобы сотрудника Росфинмониторинга. «Сотрудник» сообщил ей, что на её имя оформлен кредит, а эти деньги пошли на нужды и поддержку чужой армии. Далее её соединили с «сотрудником ФСБ», который сообщил ей, что на девушку завели уголовное дело. Прикрывающийся Федеральной службой безопасности мошенник перезвонил

64 https://iz.ru/1886811/taibat-agasieva/podslushajte-soobshchenie-moshenniki-stali-imitirovat-svoe-razoblachenie

ей по видеосвязи: девушка увидела, что в кабинете за столом сидит мужчина в костюме, а на стене портрет президента. В процессе разговора, как рассказали в Следственном отделе бердской полиции, девушку настолько сильно запугали, что когда аферист заявил ей, что он прямо сейчас проведёт обыск по видеосвязи, то она безропотно согласилась. Свои слова он подкрепил демонстрацией постановления о возбуждении уголовного дела. Бердчанка прошлась с телефоном по квартире и сняла неизвестному человеку всё, что в ней имеется, включая наличие ювелирных украшений.

Дальше девушка села в такси, которое ей вызвали аферисты, сдала все имеющиеся украшения в ломбард и получила за них деньги. Там, по легенде мошенников, золотые изделия должны были оценить, чтобы указать их стоимость в документах обыска, и вернуть обратно. Вырученные деньги в сумме более 100 тысяч рублей и имеющуюся наличность местная жительница положила на «безопасный счёт» в банке. Таким образом она лишилась 264 тысяч рублей».

18. Новая сим-карта

«Телефонные мошенники придумали схему, в которой обманывают россиян якобы открытой на их имя подарочной sim-картой. Мошенники для реализации схемы[65] представляются сотрудниками одного из российских мобильных операторов, сообщая абоненту об открытой на него подобной sim-карте с уже записанной суммой - к примеру, 450 рублей. Они заверяют, что, если абонент не нуждается в данной sim-карте, ее можно закрыть, а деньги - вывести на свой банковский счет. Но якобы для вывода денег им нужны персональные данные, такие, как ФИО, данные паспорта, банковской карты и так далее. Они могут также попросить установить приложение для удаленного доступа или передать

65 https://tass.ru/ekonomika/22097409

код, который приходит в SMS. А если не выполнить указанные действия сразу, то деньги будут потеряны. Получив все нужные им данные или сразу же доступ к учетным записям, телефонные мошенники получают доступ и к деньгам на счетах. В связи с этим, не нужно доверять подобным предложениям и не сообщать посторонним лицам свои личные данные».

19. СМС-бомбинг

«Аферисты начали использовать[66] техники так называемого SMS-бомбинга — это вид кибератаки, при которой массово отправляются сообщения на мобильный номер конкретного человека. Сразу после этого жертве начинают поступать звонки якобы сотового оператора, который сообщает о том, что они видят массовую SMS-атаку, и предлагает вам выход из ситуации, но через подтверждение ваших персональных данных и кодов из SMS».

Как следует из вышеперечисленных 19 схем, злоумышленники пытаются либо узнать код доступа к «Госуслугам», либо заставить жертву установить на мобильный телефон программу для его контроля. При этом узнать необходимую информацию им позволяют дополнительные уловки — например, предложение под благовидным предлогом включить демонстрацию экрана.

Во втором подходе преступники предварительно собирают досье на предполагаемую жертву, которое нередко бывает весьма подробным. Для этого используются как украденные базы данных (особенно базы, содержащие информацию из трудовых книжек), так и данные из открытых источников — например, соцсетей. В этом случае мошенничество носит

66 https://iz.ru/1750860/2024-08-30/rossiian-predupredili-o-skheme-moshennichestva-s-sms-bomberami

двухэтапный характер — на первом этапе жертве поступает сообщение от начальника (бывшего начальника, сослуживца, просто друга), в котором обычно сообщается о неких проверках со стороны российских спецслужб и настойчивой просьбой пообщаться с их представителем.

На втором этапе звонит «сотрудник ФСБ» (гораздо реже встречаются «сотрудники СКР» и других организаций) и начинает подготовку жертвы. Ей намекают, что дело серьезное, речь идет о финансировании ВСУ, но она не пострадает, если выполнит все указания. В течение нескольких дней (общающихся с жертвой преступников обычно оказывается несколько, что позволяет им работать посменно) жертву обрабатывают в стиле «добрый следователь-злой следователь» и переходят к сути схемы только после достижения полного контроля над ней. Также обязательно присутствует требование дать «подписку о неразглашении» (устную или даже письменную), что позволяет запугивать жертву уголовной ответственностью даже при попытке рассказать о разговоре ближайшим членам семьи. Часто для подавления воли жертвы ее часами удерживают на связи, угрожая расправой в случае ее прекращения.

Финалом схемы является требование перевести все средства на «безопасный счет» (обычно с помощью телефона, имеющего функцию NFC) или же, что происходит гораздо чаще, обналичить все средства и передать их с иными ценностями «помощнику следователя», в роли которого выступает дроппер.

Приведем типичные случаи:

«Расскажу свою историю, как недавно попалась на крючок мошенников. Никогда не продолжаю разговор с подобными лицами. Но недавно, я получила в Телеграм сообщение от заведующей детского сада (я уволилась 2 месяца назад). В нем она, обратившись ко мне по имени-отчеству, сообщила, что в детском саду была проверка

документов бывших и нынешних сотрудников и у проверяющего Александра Юрьевича есть ко мне вопросы, он должен со мной связаться и она просит серьёзно подойти к нашему с ним разговору.

Я спросила, а что не так с моими документами, на что она ответила, что ей ничего не известно, ее только попросили предупредить о его звонке. Я сказала, «хорошо» и почти сразу он позвонил. Голос поставлен, как у человека с погонами, речь властная и достаточно грамотная. Представился, звание свое назвал, сказал, что в саду проводилась проверка, начал задавать много вопросов, (как давно работала - уволилась, были ли конфликты у меня с заведующей и тому подобное). На мой вопрос, с какой целью спрашивает - ответил, что кто-то слил данные сотрудников нашего сада и 8 человек считаются потерпевшими, т. к. от их имени взяты кредиты от 500 т. до 1 млн., которые направлены переводом какому-то Шумейко, который числится преступником в РФ и сейчас находится на территории Украины.

Первым подозреваемым, кто слил данные считается сама заведующая, поэтому сейчас за ней ведется наблюдение, разговоры с ее телефона прослушиваются, связь с ней держать нельзя, так как это помешает следствию и назвал мне кучу статей, чтоб молчала и наш разговор не слышали третьи лица. Загрузив всем этим, перевел меня на сотрудника Центробанка, который должен помочь мне, потерпевшей стороне, аннулировать оформленный на меня кредит. Сотрудник Центробанка Дмитрий стал отрабатывать (как потом мне стало известно) старые схемы: прислал свое удостоверение, запрос у банка о взятом кредите, объяснил, что нужно взять новый кредит уже с моими данными, чтобы система банка, увидев новые данные, заблокировала кредит оформленный на украинца.

Я долго сопротивлялась, что такого не может быть и я не буду ничего делать, но то, что меня лично предупредила

заведующая и хорошо отработанное психологическое воздействие сделали свое дело... Я пошла в названный банк, чтобы оформить кредит. Дмитрий всегда висел на телефоне, инструктируя, как себя вести с сотрудниками банка и что отвечать, потому что они тоже под подозрением. Благо мне, как неработающей кредит не дали, а так как время было позднее, банки закрывались, мы договорились , что продолжим искать выход, то есть банк, который может дать мне кредит, завтра, чтобы спасти меня от мошеннического кредита.

Придя домой, я решила прошерстить интернет и как я благодарна людям, которые не ленятся и пишут о своих подобных случаях. Ситуации описаны один в один, как и у меня!

Я списалась с заведующей, спросила её ли это аккаунт в Телеграме. Она сказала - нет! А эти мошенники все-таки развели одну воспитательницу из их сада на кредит. До сих пор в недоумении, как они узнали, что я работала в этом саду и знаю Светлану Васильевну (заведующую). Ведь если бы не было от нее сообщения, я бы как обычно не разговаривала бы с ними...».

«Члена клуба «Заслуженных военных летчиков» развели на 700 тысяч рублей с помощью хитрого кода и простодушных угроз. 72-летний Владимир работает инженером и состоит в клубе «Заслуженных военных летчиков». Через него мужчину и решили обмануть по популярной в последнее время схеме. Якобы знакомый предупредил Владимира, что им, как и другими членами клуба, интересуется ФСБ. Вскоре действительно поступил звонок от силовика — бывшему военному сообщили, что от его имени якобы спонсируют ВСУ, поэтому сбережения нужно снять и отправить на проверку в ФСБ. Владимир ничего не заподозрил и продолжил общаться с мошенниками. По их указу он снял 500 тысяч рублей и передал курьеру — парню лет 18-ти — но только после специального кода «КСПН» (Командование специального назначения). В

тот же день Владимир передал другому курьеру еще 2000 евро, после чего «сотрудник ФСБ» скинул ему в мессенджере специальный документ, подтверждающий «регистрацию его финансов». Через некоторое время Владимир позвонил секретарю клуба летчиков и спросил: ну что, как там у наших дела? Оказалось, что у всех все хорошо — вот только недавно многим членам звонили мошенники и пытались развести на деньги. Тут Владимир и поник»[67].

II.2. Вовлечение в преступную деятельность

Помимо дистанционных хищений преступники активно вовлекают граждан России в противоправную деятельность. Самым распространенным здесь является предложение стать сообщником — дропом или дроппером. Такие люди необходимы мошенникам для вывода денег за рубеж, дополнительной обработки жертвы, технического обеспечения подмены номеров.

«По словам зампреда ЦБ Ольги Поляковой, каждый месяц около 80 тыс. человек, включая иностранцев, становятся дропперами — подставными участниками нелегальных схем по выведению средств с банковских карт.

«Объемы P2P-переводов — это достаточно значительный показатель всей теневой экономики нашей страны. Дропперов привозят автобусами к банковским отделениям, где образуются две очереди: одна для получения карт, другая для закрытия счетов и вывода средств, заблокированных банками»,— сказала госпожа Полякова в ходе уральского форума «Кибербезопасность в финансах». … У Банка России есть информация почти о 700 тыс. дропов. Почти половина из них — это люди до 23 лет. Обычно они находятся в регионах,

67 https://aif.ru/incidents/chlen-kluba-zasluzhennyh-voennyh-letchikov-otdal-moshennikam-700-tys-rubley

где ниже средний уровень доходов», - цитирует представителя Центробанка России газета «Коммерсант»[68]. Впрочем, представитель «Сбера» дает более пессимистичную оценку: «Большинство людей, которых вовлекают в преступные схемы телефонные мошенники, даже не подозревают об этом. Такой информацией поделился зампред правления Сбера Станислав Кузнецов в эфире телеканала «Россия-1». По его словам, лишь 35-40% людей, которых аферисты используют для вывода украденных денег, в курсе, чем они на самом деле занимаются. Кузнецов отметил, что в Сбере научились распознавать дропов и выявлять их следы. По данным банка, на территории России около 2 млн дропов, которые продают доступ к своим картам и счетам мошенникам, в основном этим занимаются молодые люди до 24 лет»[69].

В настоящее время дропперы чаще всего выступают в роли курьеров и «помошников следователя», которые забирают у жертвы наличные деньги и иные ценности, а затем через карты, криптообменники и ломбарды переводят их в безналичный формат и отправляют за рубеж. Их доля в таких схемах может составлять до 10% от похищенной суммы.

Также к дропперам относят людей, которые «сдают в аренду» свои банковские карты и аккаунты в соцсетях, часто не имея представления, для чего они на самом деде понадобились «арендатору». Некоторые дропперы используются для обучения пожилых жертв — они помогают им купить смартфоны с функцией бесконтактной оплаты, ставят специальные программы, дают советы по получению кредитов. Часть дропперов составляют люди, которые помогают злоумышленникам бесплатно — из страха или же находясь в уверенности, что помогают российским спецслужбам.

68 https://www.kommersant.ru/doc/7516831
69 https://tass.ru/ekonomika/24250671

Суть схемы: мошенники вербуют молодых людей, которые должны получать деньги у обманутых граждан и переводить средства на счета и криптокошельки аферистов. Горе-курьеров мошенники находят на сайтах и в чатах для поиска работы.

Мошенники убеждают жертву, что работа безопасна и легальна, могут предоставить фальшивые документы и удостоверения. В качестве легенды могут использовать необходимость помощи в оперативно-разыскных мероприятиях. Отсутствие возможности перевода через стандартные системы объясняют коммерческой тайной или серым импортом.

В случае успешного расследования средства потерпевшим удается вернуть только за счет поимки дропперов (а благодаря разветвленной системе видеонаблюдения их ловят в большинстве случаев). В некоторых случаях получается возместить ущерб полностью — принятые правоохранителями меры затрудняют вывод средств, особенно через ломбарды. В связи с этим обстоятельством жертвы мошенничества должны незамедлительно обращаться в правоохранительные органы.

«Полузащитник медиафутбольного клуба Fight Nights и бывший футболист сборной Азербайджана Абдулла Абациев арестован по делу о мошенничестве. Предварительно, его подозревают в разводке пенсионера на 14 миллионов рублей.

По данным Sport Baza, 31-летний Абациев был задержан 24 января. Преступление, по которому задержали Абациева, произошло ещё 15 января. В тот день мошенники начали названивать 79-летнему Владимиру П. Представляясь сотрудниками Мосэнергосбыта, ФСБ и Росинформмониторинга, они убедили пенсионера отдать курьеру 14 миллионов рублей.[70]»

Предварительно, Абациев и был тем самым курьером.

70 https://www.kommersant.ru/doc/7855181

Вечером 24 января он был задержан и признался в содеянном. На него было возбуждено уголовное дело по ч. 4 статьи 159 УК РФ (мошенничество, совершённое группой лиц в особо крупном размере). 27-го числа он был арестован Преображенским районным судом.

Абдулла Абациев — азербайджанский футболист, в том числе выступавший за различные российские клубы. В 2014 году он провёл матч за сборную Азербайджана против США.

Самым опасным и редким видом дропперов являются операторы сим-боксов (симбанков, симпулов, сим-шлюзов) — приборов, которые позволяют подменять иностранные номера мобильных телефонов на российские. Данные устройства требуют как минимум сотен сим-карт, которые также активно скупаются дропперами. В случае отсутствия работающего сим-бокса на какой-либо территории мошенники лишаются возможности совершать звонки с мобильных или якобы стационарных телефонов и в их распоряжении остаются только мессенджеры. Впрочем, и с ними удается все успешней бороться.

«Сотрудники Управления уголовного розыска ГУ МВД России по г. Санкт-Петербургу и Ленинградской области задержали еще троих подозреваемых в содействии зарубежным телефонным мошенникам.[71] Как сообщалось ранее, криминальная схема работала с начала текущего года. Молодые люди действовали по указанию анонимных кураторов. В арендованной квартире они разместили специальные технические устройства – GSM-шлюзы. Участники группы обеспечивали бесперебойную работу сим-карт операторов сотовой связи. Также в целях конспирации регистрировали их на иностранных граждан или несуществующих лиц. По указанию мошенников на абонентские номера данных сим-карт доверчивые

71 https://russian.rt.com/russia/news/1479882-mvd-zaderzhalo-telefonnye-moshenniki

граждане переводили денежные средства. Впоследствии они обналичивались или конвертировались в криптовалюту.

В ходе проведения дальнейших мероприятий оперативники установили личности еще троих подозреваемых. Двое из них проживали в Республике Дагестан, еще один – в г. Санкт-Петербурге. Они задержаны по местам жительства. В ходе обысков обнаружены и изъяты смартфоны, банковские карты и электронные носители информации. В Ленинградской области полиция раскрыла массовые поставки сим-карт для использования в схеме дистанционных мошенничеств, сообщило МВД в телеграм-канале.

Преступную схему организовал житель Всеволожского района, руководитель компании — мультибрендового дилера операторов мобильной связи. В даркнете он нашел объявление о закупке активных российских номеров call-центрами на Украине, рассказали в ведомстве. Используя сеть арендованных торговых объектов, злоумышленники получали от операторов связи партии сим-карт. Имитируя легальные продажи, их активировали, внося в биллинговые системы фиктивные данные о владельцах — иностранных гражданах. С января 2024 года участники нелегального бизнеса реализовали более 32,5 тыс. сим-карт, с помощью которых обманывали россиян. Ежедневно им поступало более 15 тыс. звонков от зарубежных call-центров»[72].

В настоящее время Банком России и МВД России принимаются меры противодействия дроперской деятельности. Организован обмен информацией об операциях, совершенных без согласия клиентов. Это позволяет кредитным организациям блокировать операции по банковским счетам, на которые поступили похищенные денежные средства. Кроме того, владельцы таких счетов лишаются дистанционного управления всеми своими счетами во всех банках.

72 https://мвд.рф/news/item/58460899

Меняется ситуация и на рынке криптовалюты, которая является важным средством анонимизации похищенных денежных средств. В ходе досудебного производства сотрудники МВД научились получать информацию о владельцах криптокошельков, проведенных по ним транзакциях и отсутствие на территории России криптобирж не является препятствием к этому, поскольку иностранные биржи предоставляют сведения по электронной почте.

Гораздо реже дропперов в преступном мире встречаются люди, которые согласились заработать деньги на диверсиях и и терактах. Особенно пострадали от этого релейные шкафы на железных дорогах, более сотни из которых были подожжены злоумышленниками.

«За прошедший год в Российской Федерации был зарегистрирован двукратный рост случаев поджогов на объектах железнодорожного транспорта. Такую информацию предоставило управление на транспорте Министерства внутренних дел России по Центральному федеральному округу, подводя итоги работы за 2024 год. В результате проведенных расследований сотрудникам полиции удалось задержать 61 человека», - сообщило информагенство ТАСС со ссылкой на МВД[73].

Помимо релейных шкафов, за поджог которых украинские кураторы обычно предлагают от 8 до 15 тыс. рублей, страдают и более серьезные объекты — автотранспорт сотрудников Минобороны, тепловозы, подстанции, вышки сотовой связи и административные здание. Наибольший финансовый урон из этого нанесло уничтожение трех вертолетов — в Подмосковье, Ямало-Ненецком АО и Челябинске с суммарным ущербом более одного миллиарда рублей. «2-й Западный окружной военный суд вынес приговор фигурантам дела о поджоге в апреле 2024

73 https://www.ridus.ru/v-rossii-za-god-udvoilos-kolichestvo-podzhogov-na-zheleznodorozhnyh-obektah-552791.html

года вертолета в подмосковном аэропорту Остафьево по заказу украинских спецслужб. Четверо молодых людей и девушка осуждены на сроки от 12,5 до 18 лет лишения свободы. … В ходе судебного процесса, который длился с февраля нынешнего года, четверо подсудимых—молодых людей признали вину частично. Они не отрицали, что сожгли релейный шкаф и вертолет, однако были не согласны с квалификацией их действий. Все фигуранты настаивали, что не были противниками СВО, а просто хотели заработать денег. Было установлено, что за диверсию на железной дороге им заплатили в общей сложности 15 тыс. руб., а за уничтожение вертолета обещали порядка 3 млн руб. В итоге за поджог «вертушки» молодые люди получили лишь 10 тыс. руб. «на расходы», - писала о самом резонансном случае газета «Коммерсант»[74].

И вот еще типичное сообщение: «Двух подростков задержали в Тверской области по делу о подготовке теракта в преддверии Дня Победы и участии в террористической организации. Двое несовершеннолетних получили указания от украинских кураторов. Они должны были совершить поджог одного из зданий Минобороны в тверском городе Вышний Волочёк. Один из фигурантов самостоятельно изготовил в нежилой постройке города зажигательные устройства. Второй подросток получил сведения о местонахождении уже изготовленных устройств. Действия молодых людей пресекли силовики»[75].

Самым же опасным видом дистанционных преступлений стали террористические атаки. Именно дистанционно украинские спецслужбы смоги завербовать исполнителей теракта в Crocus City Hall.

«22 марта 2024 года в подмосковном Красногорске перед началом концерта рок-группы "Пикник" в Crocus City Hall

74 https://www.kommersant.ru/doc/7657935

75 https://tass.ru/proisshestviya/24015027

ворвались несколько мужчин и открыли огонь по посетителям и персоналу. В здании возник пожар. «В результате указанных действий погибли 147 человек, получили телесные повреждения - 336. Причиненный ущерб составил 5,7 млрд рублей. Кроме того, три человека пропали без вести», - напомнила Генпрокуратура.

В СКР ранее сообщали, что шестеро выходцев из Средней Азии заочно арестованы и объявлены в розыск по обвинению в организации этого теракта. Как считает следствие, эти лица "завербовали четверых исполнителей нападения - Далерджона Мирзоева, Мухаммадсобира Файзова, Шамсидина Фаридуни и Саидакрами Рачабализоду - и организовали их обучение за границей".

Эти четверо и еще 15 фигурантов (Шахромджон Гадоев, Зубайдулло Исмоилов, Хусейн Хамидов, Мухаммад Зоир Шарипзода, Якубджони Давлатхон Юсуфзода, Назримад Лутфуллои, Джумахон Курбонов, Хусен Медов, Джабраил Аушев, Алишер Касимов, Умеджон и Мустаким Солиевы, Исроил Исломов, Диловар и Аминчон Исломовы), по которым расследование завершено, обвиняются в теракте, содействии террористической деятельности, прохождении обучения в целях осуществления террористической деятельности и других преступлениях.

«Следствием установлено, что это бесчеловечное преступление было спланировано и совершено в интересах действующего руководства Украины с целью дестабилизации политической ситуации в нашей стране. Кроме этого, ряд обвиняемых планировали совершить подрыв развлекательного комплекса в городе Каспийске республики Дагестан, однако это преступление было предотвращено», - сообщала представитель СК Светлана Петренко.

По ее словам, подготовка к теракту «началась за несколько месяцев до его совершения». «Часть фигурантов прибыла в Россию из-за рубежа, где они проходили первоначальную

подготовку. Ряд лиц находились на территории России и осуществляли приискание средств и орудий для совершения преступления. Другие фигуранты на постоянной основе осуществляли переделку огнестрельного оружия и, осознавая, что оно не может быть использовано в мирных целях, передали его членам террористической организации», - сказала представитель СКР.

После этого, отметила она, оружие было перевезено в Каспийск, откуда и было доставлено в Московский регион непосредственно перед терактом."После совершенного преступления его исполнители попытались скрыться на Украине, но были задержаны на территории Брянской области и доставлены в Москву. Некоторые пособники получили указания от организаторов покинуть территорию России, однако были задержаны при попытке пересечения границы", - сказала представитель СКР»[76].

Известны и такие случаи: «Второй западный окружной военный суд приговорил к 29 годам лишения свободы гражданина России и Италии Руслана Сидики (внесен в российский перечень экстремистов и террористов), который взорвал железную дорогу в Рязанской области в 2023 году. Из-за этого были повреждены 300 м пути между станциями Рыбное и Блокпост, с рельс сошли 19 вагонов товарного состава, перевозившего удобрения. Ущерб от взрыва оценили в 70 млн руб. На одном из допросов мужчина рассказал о попытке атаковать военный аэродром Дягилево в июле того же года. Третий теракт также должен был произойти на железной дороге в Рязанской области»[77].

От рук «дистанционных террористов» в России погибли генералы Игорь Кириллов и Ярослав Москалик, которые были подорваны рядом со своими домами.

76 https://www.interfax.ru/russia/1033933

77 https://www.kommersant.ru/doc/7752687

Самой безобидной преступной деятельностью в сфере дистанционных преступлений такого рода является нанесение граффити с символикой запрещенных в России украинских террористических организаций (чаще всего «Легиона «Свобода России») или же фотографирование на фоне значимых объектов (например, памятников) с распечатками их лозунгов. Впрочем, такого рода задания часто даются с целью проверки лояльности агента и сбора на него компромата, после чего поступают требования перейти к диверсиям и терактам.

П.3. Доведение до самоубийства

В конце 2015 года после резонансного самоубийства Рины Паленковой (Ренаты Камболиной) из Уссурийска в России заговорили о феномене «игр смерти» в социальных сетях, которые стимулируют подростков к самоубийствам. Широкое обсуждение этой темы началось с публикации статьи журналистки «Новой газеты» Галины Мурсалиевой «Группы смерти (18+)», которая вышла 16 мая 2016 года. Она начиналась с таких слов: «Мы насчитали 130 (!) суицидов детей, случившихся в России с ноября 2015-го по апрель 2016 года, – почти все они были членами одних и тех же групп в интернете. Новые смерти анонсированы там же»[78].

В статье, ставшей пусть и не слишком точным, но первым исследованием данного феномена, содержалось важное наблюдение насчет характера суицидальных игр – «как будто там те же люди, что и в закрытых группах «ВКонтакте», которые без конца повторяют: «Чем больше суицидников – тем меньше суицидников и их близких». Или вот еще: «Чем больше нестабилов выбракуется от подросткового суицида, тем легче будет жить». Это явно фашистская матрица, но тема подросткового суицида, конечно, и правда всегда стояла остро».

78 https://novayagazeta.ru/articles/2016/05/16/68604-gruppy-smerti-18

Действительно, «игры смерти» оказались вполне фашистским изобретением. Точнее, укрофашистским.

20 марта 2017 года уполномоченный по правам ребенка при президенте РФ Анна Кузнецова заявила, что в 2016 году уровень числа детских самоубийств в России вырос на 60%. В целом же, если с 2011 года наблюдалась положительная динамика по снижению количества самоубийств в нашей стране на 10%, то в 2016 году число таковых выросло на 57%.

«Мы резко откатились назад на пять лет. Одной из основных причин такого положения является лавинообразное распространение «групп смерти» в соцсетях», – заявила она на селекторном совещания «О профилактике суицидов среди несовершеннолетних» в ГУ «Национальный центр управления в кризисных ситуациях» МЧС[79]. С учетом общего количества таких суицидов (720 в 2016 году), рост на 57% мог привести к гибели более 200 людей по вине «игр смерти». Мы обладаем сведениями только по тем несчастным детям, которые фактически были убиты дистанционно чужими руками, (когда) ребенок находится в состоянии безысходности, им манипулируют и им управляют», – добавила она. Вице-спикер Государственной Думы РФ также отметила, что в 2015 году, по данным СК, в 32 субъектах РФ существенно по сравнению с 2014 годом увеличилось количество несовершеннолетних, погибших в результате самоубийства. Ведется война против детей, настоящая преступная деятельность, очень продуманная, организованная, целенаправленная и имеющая последствия», – добавила она[80].

В свою очередь, директор Лиги безопасного интернета Денис Давыдов уточнял, что «группы смерти» – это часть информационно-психологической операции (ИПО), которая проводится против нашей страны. «Мы считаем, что это

79 Источник: https://ria.ru/20170320/1490383656.html

80 https://lenta.ru/news/2017/02/13/yarovayasuicide/

такое тестирование информационного оружия в отношении подростков, в отношении наших граждан в целом. Способы вовлечения детей и подростков в эти группы, эти игры, схожи со способами вовлечения и вербовки деструктивными религиозными культами. Знание возрастной психологии, использование информационных технологий, конечно, говорит о четкой, спланированной и скоординированной работе. Кто эту работу проводит, к сожалению, в настоящее время сложно сказать. Мы считаем, что это спланированное тестирование такого вида информационного оружия. И понятно, что здесь действуют не какие-то сумасшедшие одиночки или просто сектанты. Скорее всего, к этому причастны враждебные силы по отношению к нашей стране», – заявлял он[81]. Аналогичной позиции придерживался и руководитель Центра кризисной психологии Михаил Хасьминский.

В феврале 2017 года на слушаниях в Общественной палате менеджер по интернет-маркетингу ПАО «Мегафон» Антон Елизаров заявил, что за управлением «групп смерти», которые известны еще как «суицидальные паблики», стоят украинские националисты[82].

«Московская полиция продолжает расследование по так называемым «группам смерти», они же группы «синий кит». Напомним, в соцсетях за последний год начали появляться такие страницы, которые активно пропагандировались среди подростков. Участникам групп «киты» давали различные задания. Финальный уровень – «самоликвидация». Серией самоубийств и попыток, которые не удалось – слава богу – довести до конца, занимаются в Следственном комитете и полиции. Специалистам удалось вычислить IP-адреса компьютеров кураторов «синих китов». Часть из них общалась с российскими подростками с территории Украины.

81 http://novorusmir.ru/archives/22558

82 https://www.kommersant.ru/doc/3221027

– Это уже достоверно установлено, – рассказал «КП» источник, близкий к следствию. – Компьютеры, с которых осуществлялось управление некоторыми группами «синих китов» физически находятся в Харьковской и Винницкой областях, Киеве. Часть групп оперативно удалялись сразу после того, как поступали сигналы о «самоликвидации» подростков, с которыми они «работали».

По словам источника, информация об IP-адресах «китов» передана в правоохранительные органы Украины с просьбой помочь в задержании указанных лиц. Но, судя по всему, кураторы уверены в собственной безопасности. Например, они охотно переписываются с так называемыми «антикитами» – активистами, которые в Интернете борются с «группами смерти» и отговаривают подростков от опрометчивых шагов.

– В этих сообщениях они открыто признают: да, мы находимся на Украине, – сообщил «Комсомолке» один из активистов», – со ссылкой на полицию писала об этом «Комсомольская правда»[83].

26 февраля 2020 года свою позицию по данной теме высказал и Президент России. «В поле вашего постоянного внимания должно находиться интернет-пространство, в котором продолжают действовать разного рода радикальные группы, пропагандирующие уголовную субкультуру, склоняющие подростков к самоубийствам, к совершению правонарушений. Работа по их выявлению должна вестись постоянно, а организаторы и подстрекатели – нести заслуженное наказание», – заявил В. Путин на заседании коллегии МВД.

После комплекса мер, предпринятых российскими правоохранителями, проблема дистанционного доведения до самоубийства стала менее острой, но с повестки дня не ушла. До сих пор российские дети продолжают погибать в результате

83 https://www.msk.kp.ru/daily/26672/3694869/

«игр смерти» и иных способов воздействия на психику. Вот, например, выдержка из прошения на имя православного митрополита с просьбой разрешить отпевание погибшей девочки: «Девочке было 11 лет, она выбросилась с 8 этажа. В предсмертном сообщении сказала, что давно об этом мечтала и хочет узнать, что на том свете. Никаких психиатрических диагнозов не имела. На данный момент идут следствие и посмертная психиатрическая экспертиза. Предполагают внешнее влияние.».

Со временем проблема дистанционного доведения до самоубийства перекинулась и на взрослых. Немало жертв дистанционных хищений, лишившиеся всего имущества или же потерявшие доброе имя, покончили с собой. Бывшая судья Таганского суда Москвы Наталия Ларина (отдала мошенникам 2 млн.), профессор МГУ Борис Бояринцев (потерял 50 млн.), врач Павел Ощепков (перевел мошенникам миллион) и сотни других людей именно так закончили свою жизнь[84].

«Пойманы трое мошенников, которые причастны к доведению до самоубийства 17-летнего юноши отдавшего телефонным мошенникам отцовские 500 тыс. рублей. Напомним, что 7-го февраля под окнами дома 25/4 по проспекту Культуры был найден труп несовершеннолетнего парня. Выяснилось, что ещё 5-го февраля с ним связались телефонные мошенники и уговорили его перевести им свыше 500 тыс. рублей, которые принадлежали его 68-летнему отцу. В конечном итоге, не выдержав мук совести, подросток решил покончить жизнь самоубийством. Сегодня пришло сообщение, о том, что в Барнауле задержаны трое друзей от 21 до 24 лет, которые работали на "организацию" из-за рубежа (прозвон осуществлялся там, а парни выполняли необходимые задачи на местах). Один из задержанных искал людей, которые за деньги соглашались оформлять на своё имя карты и симки

84 https://www.kommersant.ru/doc/6747861

— на них жертвы в итоге и переводили деньги. Далее средства выводились и улетали начальникам процесса через крипту. В квартирах троицы провели обыски и изъяли 34 банковские карты и 11 мобильников — в одном из них и была переписка со студентом из Питера, который вскоре после перечисления денег мошенникам не выдержал и совершил самоубийство»[85].

А вот выдержка из одной деструктологической экспертизы: «согласно материалам дела, N находился под психологическим воздействием мошенников около месяца. Сначала ему позвонил сотрудник ПАО «Сбербанк России» из г. Москвы и сообщил, что его квартира продается на «электронном аукционе», сообщили, что против N орудуют дистанционные мошенники, предложили схему по «возвращению квартиры», которую на самом деле никто не продавал. Преступники сообщили, что необходимо продать квартиру быстрее мошенников, давили на него, поэтому мужчина вскоре лишился жилплощади. Также после продажи квартиры мошенники заставили N совершить попытку поджога военкомата, «чтобы вернуть квартиру». После поджога N был задержан правоохранителями и помещен под домашний арест. Вскоре он повесился». Таким образом, здесь пенсионер стал жертвой дистанционного хищения, был вовлечен в преступную схему как исполнитель и в итоге доведен до самоубийства.

Существуют и другие способы дистанционно убить людей. «Первокурсник Московского физико-технического института (МФТИ) Петр Ветчинкин совершил самоубийство под давлением «мошенников-ВСУшников», добивавшихся от него совершения теракта. Об этом сообщается на странице студента в социальной сети «ВКонтакте». По словам авторов поста, молодой человек скончался 21 декабря 2024 года.

85 https://mr-7.ru/articles/2025/02/23/v-barnaule-zaderzhali-troikh-moshennikov-po-podozreniiu-v-prichastnosti-k-samoubiistvu-17-letnego-peterburzhtsa-news

Мошенники, которые, как утверждается, связаны с ВСУ, «терроризировали» Ветчинкина по телефону в течение шести часов, «навешивали» на него кредиты, писали недостоверные письма о том, что он якобы состоит в экстремистской организации, а также угрожали расстрелом его семьи и близких людей. «Он мужественного пытался разобраться со всем один. Мошенники довели его до самоубийства. 27.12.24 состоялись похороны», — сказано в сообщении»[86].

Кроме вышеперечисленных схем дистанционного доведения до самоубийства имеет смысл коснуться и темы биодронов, более подробно рассматриваемой в следующем разделе. Дело в том, что при совершении диверсий и терактов биодроны обычно используют зажигательные смеси, от которых нередко страдаю сами, получая ожоги вплоть до летальных. Приведем классический случай: «В Воронеже умерла девушка, которая подожгла два кафе по указке мошенников. Утром 29 января 20-летняя София Белявцева зашла в кафе Buntaro на Плехановской улице, достала бутылку с зажигательной смесью, облила мебель и подожгла. В этот момент в кафе находилась другая посетительница, а также сотрудница. Троих девушек госпитализировали — все они получили ожоги. Больше всех пострадала сама Белявцева: она получила ожоги 90% тела. В телефоне девушки следователи нашли переписку с неизвестными, которые и приказали ей поджечь заведение. Позже оказалось, что за день до поджога Buntaro на Плехановской София подожгла заведение той же сети в парке «Алые Паруса». Белявцева находилась в реанимации 14 дней. Врачи боролись за её жизнь, но сегодня девушка скончалась. У 22-летней сотрудницы кофейни диагностировали ожоги 40% тела, третью девушку доставили в больницу с 20% ожогов. Они находятся под наблюдением врачей»[87].

86 https://ria.ru/20250110/moshenniki-1993172606.html
87 https://t.me/bazabazon/34688

Таким образом, общее количество погибших вследствие такого рода схем россиян может достигать одной тысячи человек.

II.4. Феномен биодронов

После начала СВО в 2022 году криминологи столкнулись с новым видом преступников, которые одновременно являлись и потерпевшими. Сотни жертв дистанционных хищений оказались настолько внушаемыми, что под влиянием преступников согласились на совершение терактов, диверсий и иных преступлений. При этом «потерпевшие-преступники», получившие название биодронов, пребывали в уверенности, что участвуют в операциях российских спецслужб и бесплатно помогают ловить злоумышленников. Это обстоятельство принципиально отличает их от дропперов, поджигателей релейных шкафов и прочих преступников, которые совершали правонарушения за деньги и обычно знали, кто является их реальными заказчиками.

Самыми распространенными преступлениями биодронов стали поджоги военкоматов, отделений банков, автотранспорта и нападения на избирательные участки. Из более редких случаев можно отметить поджоги школ, гостиниц, поликлиник, ресторанов, торговых центров и православных храмов. В большинстве случаев эти эпизоды были квалифицированы как теракты, что повлекло за собой осуждение биодронов на соответствующие сроки лишения свободы.

Вот типичная новость: «в Челябинской, Ивановской и Тульской областях задержаны четверо россиян, которые, будучи обманутыми телефонными мошенниками, по заданию украинских кураторов собирали для Киева информацию и совершали диверсии. Об этом сообщил Центр общественных связей ФСБ России. Как установили силовики, задержанные вели разведку, фото- и видеосъемку объектов

транспортной и энергетической инфраструктуры регионов, поджигали автомобили сотрудников правоохранительных органов и повредили опоры высоковольтных ЛЭП. Как заявили сами задержанные, они попали под влияние телефонных мошенников, переведя на "безопасные счета" от 250 тысяч до полутора миллионов рублей, после чего с ними через Telegram и WhatsApp (***принадлежит Meta, признанной экстремистской и запрещенной в РФ***) связались неизвестные. Они представились сотрудниками правоохранительных органов и под угрозой уголовного преследования за финансирование ВСУ склонили россиян к преступлениям, которые назвали «участием в проверке антитеррористической защищенности объектов». На фоне этого в ФСБ России в очередной раз напомнили об активности украинских спецслужб в интернете, в частности в соцсетях, ради вовлечения граждан в противоправную деятельность. «Пользуясь их доверчивостью, вербовщики принуждают своих жертв совершать тяжкие и особо тяжкие преступления, за которые предусмотрены длительные сроки заключения», - предупредили в ЦОС»[88].

«После начала боевых действий на Украине в России появилась новая категория преступников — те, кто совершил действия условно террористической направленности под воздействием мошенников, обманувших или запугавших человека. В такой обман бывают втянуты наиболее уязвимые люди — подростки и пожилые. Мошенники выдают себя за сотрудников спецслужб, банков, органов власти, заставляя людей поджигать релейные шкафы, военкоматы, здания администраций. Кого-то они убеждают «помочь Родине», кого-то загоняют в долговую яму с помощью кредитов, и «единственный способ» из нее выбраться – выполнить задание.

88 https://rg.ru/2025/07/07/chetvero-rossiian-zaderzhany-v-treh-regionah-rossii-za-diversii-po-zadaniiu-ukrainy.html?tgm

На проблему, при которой тех преступников, которые осознанно совершили теракт, и тех, которые считали, что помогают Родине, судят по одной и той же статье, давая им, соответственно, сроки в одном диапазоне, обратил внимание ряд юристов. В частности, об этом в начале июня говорил в своем выступлении в Совете Федерации вице-президент Федеральной палаты адвокатов, президент Адвокатской палаты Москвы Сергей Зубков. «Мы все чаще и чаще видим, как по этой статье [205-й] фигурантами становятся пожилые люди, а самое неприятное — несовершеннолетние, которые втягиваются обманным путем активно действующими на территории Российской Федерации телефонными мошенниками, которые зачастую контролируются спецслужбами иностранных государств. Нам нужно совместно думать над тем, как с точки зрения правоприменения и законотворчества решать эту проблему», — заявил Зубков[89].

В то же время психиатрические экспертизы, которые были проведены в отношении большинства биодронов, показали их вменяемость. Сейчас на повестке дня стоит вопрос определения принципиально нового медицинского диагноза для лиц из этой категории, однако вряд ли этот процесс будет быстрым.

В некоторых случаях биодроны могут выступать и в роли дропперов. «92-летний пенсионер отдал мошенникам все свои сбережения, попавшись на уловку о необходимости перезаключении договора на обслуживание телефона. Испугавшись, что останется без городского телефона, мужчина продиктовал по телефону номер СНИЛС. Дальнейшие действия аферистов не отличались изобретательностью, мужчине позвонил якобы сотрудник силовых структур и сообщил, что пенсионер передал свои данные мошенникам и

89 https://www.rbc.ru/politics/04/07/2025/685409459a7947662bba4b08?from=newsfeed

теперь на его имя открыт счет в одном из банков, с которого осуществляется перевод денег в другую страну. Введенному в заблуждение пожилому мужчине постоянно звонили на мобильный и городской телефоны лжеправоохранители и сумели убедить, что все накопленные денежные средства необходимо передать курьеру для проведения «декларации».

В качестве курьера злоумышленники решили использовать обманутую ими 83-летнюю женщину, у которой они также по телефону выведали данные паспорта и СНИЛС, а затем запугивали получением на ее имя кредитов. Запутавшаяся пенсионерка согласилась оказать содействие, как она полагала, сотрудникам правоохранительных органов, и поехала по указанному ей адресу, чтобы забрать пакет у пожилого мужчины. Телефонные аферисты даже вызвали женщине такси, чтобы она съездила за «посылкой», сказав кодовое слово.

Пенсионер, следуя указаниям, передал приехавшей женщине уложенные в пакет 600 тыс. рублей, 1 тыс. Евро и 49 тыс. долларов США, при этом женщина не знала, что забирает деньги. Злоумышленники вновь вызвали «женщине-курьеру» такси, на котором она приехала в другой район, и, также следуя телефонным указаниям, отдала пакет неизвестному мужчине»[90].

Отмечаются и более сложные схемы. «Мошенники организовали целую спецоперацию, чтобы поджечь полицейский автомобиль в подмосковном Реутове. Подробности сообщает Telegram-канал Baza. 80-летнюю пенсионерку Людмилу Матвеевну уговорили сделать ложный вызов о краже шубы, чтобы вызвать полицию на место. Вторая пенсионерка, 73-летняя Нина Борисовна, поджидала полицейскую машину. Когда полицейский прибыл на вызов

90 https://epp.genproc.gov.ru/web/proc_77/mass-media/news/reg-news?item=104979487

к Людмиле, Нина Борисовна подошла к полицейскому автомобилю, облила его бензином и подожгла. Очевидцы вызвали полицию. В момент задержания женщина говорила по телефону с аферистами и выкрикивала экстремистский лозунг «Слава Украине». Людмила Матвеевна, в свою очередь, призналась силовикам, что была частью плана — она сделала ложный вызов, чтобы выманить полицейского на место «происшествия». По словам журналистов, полицейская машина выгорела полностью. На поджигательницу завели дело об умышленном уничтожении имущества»[91].

Известны и совсем экзотические способы использования биодронов. «Телефонные мошенники убедили женщину войти с муляжом пояса смертника в отделение банка на Пролетарском проспекте в Москве. 36-летняя жительница Москвы угрожала сотрудникам, требовала выдать деньги и вела видеосъёмку. На её поясе находился муляж, внешне напоминающий взрывное устройство. После того как персонал отказался выполнять её требования, женщина самостоятельно покинула помещение. Она была задержана»; «Супружескую пару из Перми арестовали в Москве за пикет с плакатом «Величие СБУ». Они заявили, что их заставили мошенники. Тверской районный суд Москвы оштрафовал на 30 тысяч рублей и арестовал на 13 суток Диану Килдиарову и Раиля Хусаинова из Пермского края за пикет у выставленной военной техники с плакатом «Величие СБУ», сообщает[92] «Осторожно, новости». Суд признал их виновными в дискредитации российской армии (ч. 1 ст. 20.3.3 КоАП) и неповиновении полиции (ч. 1 ст. 19.3 КоАП). Правонарушение произошло в на 30 апреля у ограждения с военной техникой. По версии обвинения, с которой согласился суд, супруги публично выразили негативное отношение к Вооруженным силам

91 https://www.gazeta.ru/social/news/2024/12/24/24698630.shtml
92 https://t.me/ostorozhno_novosti/38324

России. По утверждению самих задержанных, сделали они это не по своей воле, а потому что стали жертвами мошенников, которые якобы заставили их взять кредит, оплатили поездку в Москву и под угрозами вынудили выйти на акцию»[93].

Самым дерзким преступлением биодронов стал поджог двери общественной приемной ФСБ России. «Стало известно, что московский студент по имени Никита поджег дверь в здании Федеральной службы безопасности на Лубянской площади в столице по подстрекательству злоумышленников. 18-летний студент Государственного университета спорта и туризма был уверен, что принимает участие в неких учениях, проводимых спецслужбами, и только после нескольких часов на допросе в правоохранительных органах понял, что никаких учений не было»[94].

В настоящее время в России выявлено не менее 500 биодронов, преимущественно пожилого возраста. С учетом их специфической мотивации для совершения преступлений выдвигаются предложения о смягчении наказания. «Должно быть четкое разграничение умышленной террористической деятельности, когда человек прекрасно осознает, чем он занимается, и стремится к тому, чтобы причинить вред людям, обществу, государству, и действий, когда обманутый гражданин делает что-то, но не понимает, что втянут в совершение преступления, а его потом рассматривают наравне с настоящим террористом. Это неправильно», - полагает цитировавшийся выше вице-президент ФПА Сергей Зубков, однако многие его коллег такой подход не приветствуют[95].

93 https://mos-gorsud.ru/rs/tverskoj/services/cases/admin/details/2b8569b0-25b4-11f0-be58-1ff0550ef590

94 https://yamal-media.ru/news/podzhog-dveri-v-zdanii-fsb-v-moskve-zaderzhan-student-kolledzha

95 https://www.rbc.ru/politics/04/07/2025/685409459a7947662bba4b08?from=newsfeed

С целью определения возможности привлечения жертв дистанционных мошенников к уголовной ответственности за содеянное или же установление необходимости применения к ним принудительного лечения, получения ответа на вопрос, виновны ли эти лица, и должны ли они понести наказание, либо психологическое воздействие на них было столь сильным, что они не смогли этому противодействовать, по инициативе Следственного департамента МВД Россиив НМИЦ психиатрии и наркологии им. В.П. Сербского для органов предварительного расследования в системе МВД России проведен большой объем (более 90) судебных психолого-психиатрических экспертиз в отношении жертв дистанционных мошенников.

Такая потребность возникла в связи с тем, что способы совершения дистанционных хищений кардинально изменились. Фактически человек стал инструментом совершения преступлений. Причем как для хищения денежных средств, так и для подрыва государственного строя.

По ряду расследованных уголовных дел, согласно выводам проведенных биодронамкомплексных психолого-психиатрических экспертиз установлено, что последние нуждались в применении к ним принудительных мер медицинского характера, что свидетельствует о том, что зачастую лица, совершаемые поджоги несут опасность для общества.

Необходимы новые методы и тактика расследования подобных видов преступлений, позволяющие определить мотивы и эмоции, которые движут людьми во время совершения преступлений по указанию социальных инженеров, в том числе об использовании человека в качестве инструмента экстремистской и террористической деятельности, поскольку они лежат в основе субъективной стороны состава преступления. Требуется дальнейшее исследование данного феномена, так как от действий биодронов зависят судьбы других людей.

Глава III. Направления деятельности по профилактике и противодействию дистанционным преступлениям.

III.1. Нормативно-правовые и технологические направления противодействия дистанционным преступлениям

Для противодействия дистанционным преступления используются в комплексе нормативно-правовые подходы и меры технической борьбы.

Распоряжением от 30 декабря 2024 года №4154-р Правительство России утвердило «Концепцию государственной системы противодействия преступлениям, совершаемым с помощью информационно-коммуникационных технологий». «Защита государства, общества и граждан от мошенников, использующих цифровые технологии, разработка правовых и технических мер противодействия таким правонарушениям, создание специальных подразделений для расследования такого рода преступлений – эти и другие цели изложены в Концепции государственной системы противодействия противоправным деяниям, совершаемым с помощью информационно-коммуникационных технологий. Распоряжение о её утверждении подписал Председатель Правительства Михаил Мишустин.

Согласно документу, одной из важных частей государственной системы должна стать специализированная цифровая платформа, обеспечивающая оперативный обмен информацией между правоохранительными органами, Центральным банком, кредитными организациями и операторами связи для установления всех обстоятельств и лиц, причастных к мошенническим действиям.

Противодействие ИТ-преступлениям необходимо вести по трем направлениям: законодательное (существующие законы должны отвечать современным условиям жизни общества),

технологическое (компаниям, осуществляющие обработку персональных данных должны обеспечить эффективную защиту информационных баз) и профилактика преступлений (население должно быть осведомлено о существующих угрозах, порядке оказания и получения дистанционных услуг, работе правоохранительных органов).

Кроме того, на региональном и муниципальном уровнях должны быть приняты соответствующие целевые программы по профилактике правонарушений и преступлений, совершаемых с использованием цифровых технологий.

Концепция также предусматривает создание механизма оперативной приостановки операций с денежными средствами, использовавшимися в преступной деятельности.

Ещё одно направление работы – совершенствование уголовного законодательства, в котором должны появиться новые определения видов преступлений, совершённых с использованием информационно-коммуникационных технологий.

Особое внимание в концепции уделено повышению уровня осведомлённости граждан, в первую очередь пожилых, о методах мошенников и способах защиты от их действий. Для этого предлагается размещать социальную рекламу, цель которой – сформировать у граждан цифровую грамотность. К участию в такой социальной рекламе необходимо привлекать известных представителей культуры, науки и информационного сообщества.

План мероприятий по реализации концепции в шестимесячный срок поручено разработать МВД совместно с заинтересованными органами власти при участии Генпрокуратуры, Следственного комитета и Банка России.

Создание системы эффективного противодействия преступлениям, совершаемым с помощью информационно-коммуникационных технологий – один из показателей достижения национальной цели развития «Цифровая

трансформация государственного и муниципального управления, экономики и социальной сферы». Этот показатель был утверждён соответствующим указом Президента в мае 2024 года», - говорится в пояснении на сайте Правительства[96].

Затем был принят Федеральный закон от 01.04.2025 N 41-ФЗ "О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации"[97].

Основными его позициями стали:

- обязанность банков принимать меры к приостановлению операций по получению денежных средств с использованием банкоматов;

- возможность назначения уполномоченного лица для подтверждения операций с денежными средствами;

- период охлаждения к выдаче кредитов, ужесточены требования к идентификации клиентов (ЕСИА, биометрия), сокращены сроки обмена информацией с Бюро кредитных историй, обязательная биометрия;

- проработан механизм Антифрода для предотвращения несанкционированного доступа к личным кабинетам Госуслуг (ограничение подозрительной активности на 72 часа, тестовый режим входа в личные кабинеты в тестовом режиме);

- введено понятие сим-бокса и установлены ограничения по его использованию;

- регламентирован порядок осуществления массовых вызовов и возможность абонентов отказаться от них;

- установлен запрет на передачу сим-карт.

96 http://government.ru/docs/53922/; http://static.government.ru/media/files/AVixvkRaPxG3ZXDca0ShH3LexTiMMMsD.pdf

97 http://www.kremlin.ru/acts/bank/51783

Далее был принят «Закон о внесении изменений в статью 187 Уголовного кодекса Российской Федераций» от 24 июня 2025 года[98].

Поправки были внесены в статью 187 УК России (неправомерный оборот средств платежей). Они устанавливают, что лицо, передавшее из корыстных побуждений другому человеку свою банковскую карту или доступ к ней для совершения неправомерных операций, понесет наказание в виде штрафа до 300 000 рублей или в размере своего дохода за период от трех месяцев до года, или обязательных работ до 480 часов. Также на него может быть наложено наказание в виде исправительных работ (до двух лет), принудительных работ (до трех лет) или ограничения свободы на тот же срок.

Также стоит отметить Федеральный закон «О внесении изменения в статью 26 Федерального закона «О банках и банковской деятельности» от 24 июня 2025 года («Закон о родительском контроле за счетами подростков для защиты от мошенников»), усиливающий защиту несовершеннолетних (14-18 лет) от вовлечения в преступную деятельность. Теперь родители или законные представители получили право запрашивать справки по банковским счетам и вкладам своих детей. Закон напрямую направлен против схем, когда мошенники под видом легкого заработка вовлекают подростков в оформление карт и счетов (в 2023 году клиентами банков были 2 млн подростков)[99].

Также принят ряд дополнительных нормативных актов, которые позволили:

- *заблокировать пропуск иностранного трафика с подменой номера;*

98 http://publication.pravo.gov.ru/document/0001202506240043?index=6
99 https://sozd.duma.gov.ru/bill/579820-8#

- осуществить оперативный обмен между Банком России и МВД России и блокировать похищенные денежные средства на счетах дропов, а также приостанавливать удаленное банковское обслуживание всеми их счетами;

- установить период охлаждения по исполнению несвойственных для клиента операций, подпадающих под признаки совершенных без согласия;

- урегулировать порядок реализации сим-карт, установив лимит для одного гражданина;

- установить гражданам самозапрет на выдачу кредита,

- заблокировать оформленные и не использующиеся гражданином сим-карты;

- блокировать фишинговые сайты;

- введена уголовная ответственность за утечки персональных данных;

- установлены оборотные штрафы для компаний, допустивших такие утечки.

Также на протяжении нескольких лет принимаются различные технические меры противодействия IT-преступлениям, которые в основном направлены на блокировку входящих звонков и вывода похищенных денежных средств. Эти меры позволили впервые за три года снизить на 1% регистрацию дистанционных хищений, а в целом сократить прирост дистанционных мошенничеств с 38,2% в 2023 году до 6,8% в 2024 году.

В современных реалиях необходимо быстрое реагирование на возникающие угрозы, требуется такая организация работы, при которой необходимые для расследования сведения будут получены в режиме реального времени.

С этой целью МВД России организован электронный документооборот с банками, операторами связи, интернет-ресурсами. Также организован информационный обмен с Банком России на платформе АСОИ ФинЦЕРТ, позволяющий

оперативно приостанавливать дистанционное управление счетами, на которые поступили похищенные денежные средства.

С 1 сентября 2025 года Федеральным законом от 31 июля 2025 г. № 278-ФЗ в Уголовно-процессуальный кодекс Российской Федерации внесены изменения, наделяющие следователя с согласия руководителя следственного органа и дознавателя с согласия прокурора правом приостановления операций с денежными средствами, электронными денежными средствами, денежными средствами, внесенными в качестве аванса за услуги связи. Соответствующая мера процессуального принуждения предусмотрена статьей 1152 УПК.

Наблюдается снижение регистрации дистанционных мошенничеств, как и снижение, благодаря Антифород системам, количества мошеннических звонков с 22 млн в сутки до 7 млн. Но даже такое их количество привело к увеличению на 17% причиненного ущерба и регистрации более 154 тыс. преступлений.

Интересным экспериментом можно назвать сервис «Фрод-рулетка», запущенный летом 2024 года «Т-банком». «Фрод-рулетка» — это наш сложный экспериментальный проект, который уже на стадии раннего тестирования показывает феноменальные результаты. Я напомню, как работает сервис. Когда мы понимаем на своей стороне во время соединения, что звонок мошеннический, мы можем не отправлять его на абонента, с которым хотят связаться злоумышленники, а перевести его на «игрока» во «фрод-рулетку». Человек знает, что разговаривает с обманщиком, и не попадется на его удочку. Хотя бы элементарно потому, что мошенник в этот момент звонит совершенно другому человеку и пытается оперировать совершенно другими персональными данными. Обман человека невозможен даже чисто по техническим причинам.

Здесь на самом деле работает очень интересный принцип — «Фрод-рулетка» начала менять в корне сценарий

взаимодействия людей с мошенниками, в ее механике хищник, то есть, мошенник, сам становится добычей — он попадает в зависимость от пользователя, который теперь сам играет с преступником в кошки-мышки, причем абсолютно безопасно для себя», - утверждают представители банка[100].

А вот как отзываются об этом сервисе его пользователи: «Наверное многие в курсе, что один банк сделал антимошеннический пранк-сервис через который можно принимать звонки от мошенников вместо их жертв. В свой выходной решил лично его попробовать в образовательных целях. Скиллами опытных пранкеров не обладаю, да и не стремлюсь, поэтому эпичных записей тут не будет. Только мысли обо всём этом. Про многоуровневые схемы со взломом госуслуг, взятием кредитов, заменой контрольного вопроса и т.д. много где написано. Но в данном случае это самое начало развода, «холодный» звонок. Легенды, которые используются в данный момент распределяются примерно так:

1. 1% - Звонки из суда подтвердить получение повестки/ присутствие на слушание. Звонят не просто так, тут чётко обращаются к истцу. Из-за наличия информации о деле, всё очень правдоподобно.
2. 2% - Из архива МФЦ предлагают получить письмо которое не дошло по почте с пометкой документы или документация.
3. 5% - Замена счётчика от энергосбыта. Записывайтесь и заменят бесплатно, иначе потом за свой счёт.
4. 5% - просьба или требование(!) посетить поликлинику. Запись на флюорографию, например.
5. 10% - Из пенсионного фонда/социальной защиты. Надо посетить для написания заявление на перерасчёт неучтенного стажа.

100 https://iz.ru/1730743/video/frod-ruletka-nachala-meniat-stcenarii-s-moshennikami-khishchnik-sam-stanovitsia-dobychei

6. 80% - Продление договора на сим-карту, который закончился сегодня и карта отключится-заблокируется вот прямо сейчас, если договор не продлить. Тут все основные операторы связи. Были даже которых не слышал.

Везде за исключением последнего, под видом записи, номером талончика или очереди пытаются выудить код восстановления учётной записи на Госуслугах. В СМС написано «Не сообщать никому!», но легенда это учитывает. Забалтывают, что никому это всем, кроме них. Они первое лицо, а вы второе лицо. Вот третьим ни-ни, а им скажи. Местами могут весьма убедительно.

В варианте продления договора на обслуживание симкарты, кроме Госуслуг были попытки получить доступ к «Личному кабинету» у оператора. Вот тут возникает вопрос, зачем. Вектор атаки не понятен.

Все звонки это мошеннические колл-центры сами знаете откуда. На фоне иногда слышно как разводят других с иной легендой. За редким исключением почти никто не хэкает. Но когда начинают злиться, что ты «тупишь» переспрашивая информацию, то начинает проскакивать. Видно учатся и пытаются контролировать себя. Есть и необучаемые. Там и хэканье и гоп-стайл, как будто из юмористического скетча. Как последних держат, непонятно. Некоторые держатся за легенду до последнего, даже когда уже всё очевидно. Но они всё равно дают понять, что это я ошибся или сошёл с ума. Не исключено, что за этим идёт какая-то повторная обработка через некоторое время. Но чаще всего либо сразу отваливаются либо сыпят оскорблениями, уже не скрывая нюансов говора и тоже отлетают.

Информации у них, понятное дело, предостаточно. Все ИНН, Снилсы и т.п. В некоторых случаях есть родственные связи с адресами их регистрации. Заказы доставок еды и покупок в алко-маркетах. То есть все базы, что были слиты,

у них объединены и в постоянном доступе. Оперируя этой информацией, пытаются убедить в искренности своих намерений. Скажу так. для неподготовленного человека всё очень опасно. Про замену счётчика я даже почти поверил, хоть у меня нет квартиры в Ногинске, я там никогда не был и я вообще в тысячах километров от него. Но мне про якобы меня всё что надо уверенно рассказали. И счётчик за свои деньги менять я не хочу. А никаких чувствительных данных они не спрашивают. Это всего лишь запись. Стандартные фразы про «чей Крым или Киев?», как они любят президента РФ и всё такое им индифферентно. Могут произносить на любой лад.

Непонятно, почему до сих пор не принимаются меры, честно говоря. Госуслуги отличный удобный сервис. Но учитывая утечку всего чего только можно, единственной преградой от серьёзных убытков и полного краха для некоторых, остаются 4/6 цифр из СМС, которые с лёгкостью добываются социальной инженерией. Тут что-то надо менять[101].

«Хотелось бы поделиться тем, как прошёл мой первый день в качестве пользователя Фрод-рулетки (*т.е. программы по перехвату мошеннических звонков*). Начну с технических нюансов. Регистрация и настройка звонков проходит через чат бот секретаря Олега. Заказ звонка от мошенника так же через чат бот. В день можно принять не более 30 звонков на 1 пользователя. Мне приглашение скинули на оба моих номера, и я приняла аж 60 звонков за сегодня. Дальше немного моих личных наблюдений и статистики. Больше звонков поступало рано утром примерно с 8 до 10 по Мск. Потом поиск подходящего звонка занимал намного больше времени. Вероятно, это связано с тем, что больше людей в это время начали пользоваться сервисом. На первом месте по популярности звонки от имени операторов связи (около

101 https://pikabu.ru/story/frodruletka_11688923

35). На втором месте от имени мфц или госархива с якобы не полученным письмом на почте, которое переслали им (10 звонков). И на последнем месте сразу три вида развода. От имени МВД, с песней про доверенность. От имени поликлиники с направлением на флюорографию и от имени Энергосбыта с выездной бригадой для отключения света. По 1 звонку. Остальные звонки сразу сбрасывались, скорее всего, звонили мужчинам, а отвечала им женщина. Так же по моим наблюдениям, большая часть звонилок от имени операторов, звонят, не зная вообще никаких данных о потенциальной жертве. По имени обращались при таких звонках примерно 10 раз. Остальные просто «уважаемый абонент».

Для оптимизации противодействия дистанционным преступлениям выдвигаются следующие инициативы:

Минцифры обсуждает с операторами запрет на отправку sms во время звонка

Данная инициатива должна предотвратить возможное мошенническое воздействие на клиентов и передачу конфиденциальной информации, например, раскрытие полученных на телефон кодов. Об этом заявил глава Минцифры Максут Шадаев на межотраслевой конференции «Безопасность клиента на первом месте»[102]

К денежным переводам пожилых людей хотят привлекать доверенных лиц

Государственная дума планирует принять законопроект, согласно которому пожилые и другие социально уязвимые граждане смогут привлечь доверенное лицо для подтверждения своих переводов, однако в проект планируется внести существенное изменение. Сообщается,

102 https://www.vedomosti.ru/technology/news/2024/11/19/1076012-mintsifri-obsuzhdaet

что законодатели исключат из процедуры доверенность, чтобы убрать противоречие с Гражданским кодексом. Этот документ заменят на специальное соглашение. Так называемую «вторую руку» пожилой человек сможет привлечь, чтобы обезопаситься от воздействия аферистов, если не уверен, что сможет сам разобраться с обманом. Родственник или близкий друг, связанный с потенциальной жертвой договором, сможет подтверждать или отклонять дистанционные операции со счетами и вкладами. На это у него будет 12 часов после получения уведомления от банка. Однако это не охватит операции через систему быстрых платежей[103].

Банки предлагают разделить ответственность за хищение денег телефонными мошенниками с операторами связи

Суть инициативы сводится к тому, что операторы должны отслеживать и выявлять подозрительные звонки и сообщения, связанные с мошенничеством, и передавать соответствующую информацию банкам. Критерии определения таких вызовов и сообщений, по мнению авторов предложения, должно установить правительство.Предусматривается, что в случае перевода средств на подозрительный номер, который банк получил от оператора связи, ответственность за возврат денег клиенту будет нести банк. Если же оператор не уведомил банк о мошеннической активности и не заблокировал номер, обязанность по возврату средств возлагается на него[104].

В свою очередь, МВД России видит перспективы борьбы с мошенниками так:

«Основные направления деятельности по противодействию данному виду преступлений:

103 https://iz.ru/1775104/anna-kaledina/ne-s-toi-ruki-podtverzdenie-operacii-pozilyh-mogut-rasprostranit-na-snatie-nalicnyh

104 https://www.kommersant.ru/doc/7712385?from=main

1. Для урегулирования преступной среды необходимо объединение усилий различных государств для разработки единой концепции по криминализации деяний, наносящих вред как государственным интересам, так и нарушающих права физических и юридических лиц.

2. Необходимо рассмотреть вопрос об усилении административной ответственности операторов связи и их дилеров.

- предусмотренные статьей 13.29 Кодекса Российской Федерации об административных правонарушениях короткие сроки давности привлечения операторов связи к административной ответственности (90 суток) за нарушение требований Федерального закона «О связи» и внесение недостоверных сведений об абонентах не позволяют привлекать их к ответственности.

- не решена проблема возможности использования преступниками при совершении IT-преступлений «серых» сим-карт, оформленных на несуществующих лиц, в основном на граждан иностранных государств. Такие сим-карты используются для вывода похищенных денежных средств граждан, в том числе за пределы Российской Федерации.

- разрабатывается проект федерального закона, наделяющий следователя и дознавателя правом приостановления операций по счетам, использовавшимся в преступной деятельности, устанавливающий сроки исполнения запросов;

- в Банк России и Минцифры России направлены предложения по урегулированию оборота серых сим-карт, а также деятельности по реализации мобильной коммерции, в том числе по ограничению количества сим-карт и банковских карт на одни паспортные данные;

- МВД взаимодействует с кредитными учреждениями по возмещению ущерба потерпевшим по наложению ареста на денежные средства, находящимися на счетах дропов,

созданию возможности электронного документооборота, в том числе на базе платформы ФинЦЕРТ. Такое взаимодействие с одним из банков позволило возместить потерпевшим денежные средства в сумме более 100 млн рублей. Мы готовы продолжать и совершенствовать данную практику.

Кроме того, для вывода похищенных денежных средств также используются фирмы-однодневки. Например, в 2023 г. зарегистрировано 6991 преступление, связанное с регистрацией организаций на «подставных» лиц[105].

Можно сказать, что наблюдается незначительное количество преступлений указанной категории, однако деятельность по регистрации юридических лиц без намерения ведения предпринимательской деятельности криминализировано, установлена уголовная ответственность в соответствии со ст.ст. 1731, 1732 УК РФ),

Указанная статистика совсем несопоставима с количеством ИТ-преступлений, при совершении которых используются банковские карты дропов. В 2023 году зарегистрировано 677 тыс. ИТ-преступлений, что практически в 100 раз больше преступлений, связанных с регистрацией «подставных» юридических лиц.

Фирмы-однодневки были необходимы поскольку безналичные расчеты существовали только между юридическими лицами. Совершенствование форм безналичных расчетов сделало их доступными для физических лиц. Поэтому возникает необходимость урегулировать данную сферу. При этом передача банковской карты для вывода похищенных денежных средств, также как и передача паспорта для регистрации юридических лиц без намерения ведения предпринимательской деятельности должна стать

105 В 2017 году количество выявленных преступлений составило 1718, в 2018 году – 2661, в 2019 – 2809, в 2020 году – 2956, в 2021 году – 3164, в 2022 году – 7580, в 2023 – 6991.

наказуемым, поскольку с их помощью совершаются более тяжкие преступления.

В качестве примера можно привести теракт, совершенный в Крокус Сити Холл, оплату действий террористов производили на банковские карты, в том числе с использованием счетов, открытых на дропов».

Также сохраняются следующие проблемы:

1. Главная проблема – это утечки персональных данных.

И здесь не урегулирована ответственность посредников, обслуживающих операторов персональных данных, от которых утекают персональные данные.

2. Отсутствие регулирования Telegram-каналов и сайтов, вербующих в преступность (аренда аккаунтов, поиск курьеров).

Необходимо предусмотреть Антифрод-меры в части введения критериев для размещения объявлений с предложениями о заработке, которые позволят исключить вовлечение в противоправную деятельность.

3. Активность курьеров требует регламентации их деятельности.

Например, денежные средства могут перевозить только инкассаторы.

4. Защита от дипфейков: нужны доступные программы для маркировки дипфейк-звонков на аппаратном уровне

5. Риски в играх: дети через игровые платформы вовлекаются в экстремизм и кражи денег родителей.

Роскомнадзору усилить мониторинг игровых площадок для блоркировки. Банкам – ввести дополнительные проверки переводов на игровые платформы.

6. Не урегулирована деятельность, связанная с криптовалютой.

Законопроект о признании ее имуществом и порядке наложения ареста находится на рассмотрении, но сам порядок ее использования отсутствует. Урегулирован лишь

ее майнинг, а что делать с ней после этого? Похищенные денежные средства конвертируются и беспрепятственно уходят на криптокошельки. Трейдерство распространено, но не урегулировано и это лишает возможности привлечения их к ответственности в случаях, когда они получают похищенные денежные средства.

III.2 Профилактика дистанционных преступлений

Достигнутые в законодательной и технической сферах противодействия дистанционным преступлениям естественным образом дополняются мерами их профилактики. «Мы должны доводить до населения все актуальную информацию об этих преступлениях, полученную в ходе расследования уголовных дел. Обучение – единственный способ снизить количество жертв», - совершенно верно считает генерал-майор МВД Данил Филиппов.

Необходимо обучать цифровой гигиене все группы населения «От детского сада до пенсионеров», привлекая к данному процессу всех субъектов профилактики (школьные и дошкольные учреждения, ВУЗы, рабочие, трудовые коллективы, службы оказывающие услуги населению, пенсионные фонды и др.).

Следственный департамент МВД России рекомендовал ряду кредитных организаций включить в работу с клиентами методы контрфасцинации, которые нацелены на выведение биодронов из состояния фасцинации.

Сейчас на федеральных каналах запущено большое количество передач по доведению до граждан способов обмана и мер защиты от мошенников. Это «Антифейк», «Вован и Лексус», «Улика из прошлого», «Расследование Эдуарда Петрова», где уже примерно в каждом пятом выпуске вскрываются мошеннические уловки и способы защиты от них. Сняты документальные фильмы «Голосовая бомба:

террористическая война украинских мошенников»[106] и «Днепр на проводе»[107], а также художественный сериал «На крючке. Когда звонит мошенник»[108]. К данной теме обращается и современный зарубежный кинематограф — например, в фильмах «Пчеловод»[109] и «Грязные миллионы»[110].

Сотрудниками Следственного департамента МВД еженедельно для новостных выпусков даются комментарии по различным сценариям мошенничеств. Популярные актеры (например, Дмитрий Нагиев) снялись в рекламных профилактических роликах. Сотни статей и интервью по данной теме вышли на страницах центральной и региональной прессы.

В профилактических целях созданы десятки телеграм-каналов и пабликов в соцсетях, которые оперативно освещают как новые виды мошеннических схем, так и публикуют аудиозаписи разговоров с ними. Это «Вестник Киберполиции России»[111], «Лапша-медиа»[112], «Мошенник звонит на телефон»[113], Альянс по защите детей в цифровой среде[114] и многие другие.

Для профилактики дистанционных преступлений часто используется социальная реклама разных видов, около банкоматов нередко можно встретить картонные фигуры полицейских с предупреждениями о мошеннических схемам. К сожалению, эффект от этих мер оставляет желать лучшего — по данным МВД, 95% жертв мошенничества получали информацию о такой угрозе, но проигнорировали ее.

---

106 https://rutube.ru/video/5cdf73e141460ad3aa200c707d936118/
107 https://rutube.ru/video/7707f11bd05f4b86ae24cb303d34932c/
108 https://www.kinopoisk.ru/series/5935058/?utm_referrer=yandex.ru
109 https://www.kinopoisk.ru/film/4626783/
110 https://yandex.ru/video/preview/593343833551199084
111 https://t.me/cyberpolice_rus
112 https://lapsha.media/
113 https://t.me/mosh_zvonit
114 https://t.me/internetforkids_ru

Полезным видится тиражирование историй про спасение жертв мошенников силами неравнодушных людей. Известно немало случаев, когда случайные прохожие оттаскивали зомбированных пенсионерок от банкоматов, а таксисты отказывались вести их на встречи с дропперами. Таких людей следует поощрять по линии ФОИВов или правоохранительных органов.

Приведем типичные примеры: «В Москве прохожая спасла пенсионерку от мошенников: женщина увидела, как взволнованная бабушка ожидает такси с большим пакетом в руках и постоянно общается с кем-то по телефону. Недолго думая, женщина начала разговаривать с бабушкой и вызвала полицию.

В участке выяснилось, что подозрения женщины оказались верными. Мошенники позвонили 79-летней Ларисе Андреевне 3 марта, убедили её сказать свой номер СНИЛС, а потом перезвонили — уже с угрозами. Пенсионерку развели по стандартной схеме: «сотрудник ФСБ» убедил Ларису Андреевну, что все её средства нужно «задекларировать», чтобы её не подозревали в финансировании ВСУ. 5 марта женщина собрала все наличные, что были дома, упаковала в тряпочки и пакеты и передала неизвестной.

Звонки ненадолго прекратились, но 19 числа «силовики» убедили Ларису Андреевну выступить курьером, чтобы вернуть свои средства: ей нужно было поехать на адрес, забрать там пакет и передать его «силовикам». Бабушка согласилась и уже ожидала такси, которое ей вызвали мошенники, когда её заметила неравнодушная прохожая. Только тогда Лариса Андреевна поняла, что стала жертвой мошенников и отданные 1 855 700 рублей она уже вряд ли вернёт».

«В Красноярском крае сотрудница банка предотвратила мошенничество в отношении местного жителя. Женщина почувствовала неладное и обратилась в полицию, когда

54-летний мужчина дважды за день обратился в финансовую организацию за снятием более полутора миллиона рублей со своего личного счета и не смог пояснить для чего ему такая сумма. Мужчина рассказал, что уже два дня ему звонят якобы представители компании мобильной связи, Госуслуг и даже силовых ведомств. Сначала ему сообщили, что срок его сим-карты истекает, и нужно продиктовать код из пришедшего смс-сообщения для того, чтобы продлить договор. Затем на один из мессенджеров пришло уведомление о том, что с ним связались мошенники, и, если он озвучивал коды из смс, нужно позвонить по номеру телефона горячей линии. Позже мужчину обвинили в противоправной деятельности и обещали «посадить в тюрьму», если он не снимет все имеющиеся деньги и не переведет их на «безопасный» счет».

«В Подмосковье таксист спас пассажира от аферистов. Пассажир разговаривал в салоне авто по громкой связи - мошенники требовали положить 350 000 ₽ на «безопасный счёт» в банкомате. Водитель, услышав разговор, попытался объяснить, что того обманывают, но пассажир не поверил. Тогда таксист остановился у поста ДПС, чтобы те помогли - у них получилось убедить пассажира».

Важными видятся меры профилактики в отношении дропперов, среди которых преобладает молодежь. Эту тему следует постоянно поднимать на занятиях в средних и высших учебных заведениях, освещать на родительских собраниях и в других подходящих форматах.

Главное, что стоит доводить до слушателей на таких встречах - неотвратимость наказания для дропперов. Якобы легкий заработок такого толка неизбежно приведет не только к потере все «заработанных» денег, но и к уголовному наказанию. Это же касается и желающих помочь мошенникам через установку сим-боксов.

«В Москве завели первое уголовное дело о дропперстве. Задержана 52-летняя женщина, на чей счет злоумышленники

перевели более миллиона рублей. Подозреваемая нашла подработку в интернете. По указанию аферистов она открыла в одном из банков счет ИП, куда потом зачислялись деньги»

«С учетом позиции Пресненской межрайонной прокуратуры суд заключил под стражу мужчину, выполнявшего роль «криминального курьера» в мошеннической схеме по хищению 4 млн рублей у жительницы Москвы. 36-летнему мужчине предъявлено обвинение в совершении мошенничества (ч. 4 ст. 159 УК РФ). Вину он признал и показал, что такой криминальный заработок ему предложил знакомый, который оплатил ему дорогу из Новосибирска в Москву, сообщив, что в мессенджере ему будут приходить указания, которые надо выполнять за денежное вознаграждение. 4 декабря он по указанию соучастника распечатал присланные ему документы, приехал на ул. Большая Грузинская, где увидел пострадавшую, описание которой он ранее получил от подельника. Он подошел к женщине, назвал «кодовое слово», передал якобы банковские документы и забрал у нее пакет с деньгами в сумме 4 млн рублей, которые затем передал соучастнику. Через некоторое время обвиняемому на банковскую карту поступили 45 тыс рублей в качестве оплаты за «криминальную работу». Ранее соучастники обвиняемого позвонили 80-летней москвичке по видеосвязи с использованием технологии подмены изображения и, выдавая себя за сотрудников государственного и правоохранительного органов, убедили снять со счета 4 млн рублей и передать их курьеру для внесения якобы «на страховую ячейку», что потерпевшая и сделала», - вот такие новости весьма полезно тиражировать для подходящих целевых аудиторий.

Базовые рекомендации можно сформулировать так. «Фактически существует одно правило – никому не сообщать свои личные данные. В договорах банковского обслуживания указано: никому, даже сотрудникам банка нельзя передавать

коды доступа к управлению счетами!» А второе правило также простое – не разговаривать с чужими людьми!», - считает генерал-майор Данил Филиппов. К этому можно добавить только одно — если вам звонят от имени правоохранителей или госструктур (а такое бывает, даже если вы никому не сообщали личные данные) — требуйте личной встречи, которую мошенники обеспечить не могут.

ЗАКЛЮЧЕНИЕ

Подводя итоги настоящего исследования, посвященного проблеме дистанционных преступлений и их возрастающей роли в формировании террористической угрозы, необходимо сделать ряд ключевых выводов. Трансграничный характер современной киберпреступности объективно затрудняет прямое воздействие на организаторов и центры, зачастую находящиеся на территории других государств. В этих условиях стратегический фокус правоохранительной и превентивной деятельности должен быть смещен на внутренние уязвимости, эксплуатируемые преступными сообществами.

Первоочередной задачей становится нейтрализация низовой инфраструктуры, обеспечивающей функционирование преступных схем внутри страны. Это требует системной и бескомпромиссной работы по пресечению деятельности так называемых «денежных мулов» (дропов), их вербовщиков (дроповодов) и курьеров, отвечающих за обналичивание и легализацию похищенных средств. Одновременно с этим, необходимо купировать ключевые детерминанты, создающие благоприятную среду для данной категории преступлений. К ним относятся: практическая анонимность коммуникаций через мессенджеры, массовое использование SIM-карт, оформленных на несуществующих или подставных лиц, свободное обращение банковских карт, эмитированных

на дропов, а также отсутствие четкого законодательного регулирования оборота криптовалют, ставших идеальным инструментом для анонимизации финансовых потоков.

Вместе с тем, следует признать, что любые технологические и законодательные барьеры могут быть преодолены, пока самым уязвимым звеном в системе безопасности остается человек. Современные методы защиты информации способны эффективно противостоять техническим кибератакам, однако главной целью злоумышленников становится не взлом систем, а «взлом» человеческого сознания. Именно психологическое манипулирование, известное как социальная инженерия, лежит в основе подавляющего большинства дистанционных хищений и является инструментом для вовлечения граждан в преступную, в том числе террористическую, деятельность.

Этот факт диктует острую необходимость в глубоком криминологическом анализе, в частности, в рамках такого его раздела, как виктимология. Анализ научной разработанности проблемы выявляет парадоксальную ситуацию: несмотря на колоссальный масштаб угрозы, виктимологические исследования в этой сфере носят фрагментарный характер. Нами было установлено, что за период с 2016 по 2018 год данной теме было посвящено не более полутора сотен научных работ, причем изучению виктимного поведения как такового в них отводилось незначительное место. Глубинные социологические и психологические причины, делающие человека уязвимым для манипуляций, остаются практически неизученными. Научная проблема находится на начальной стадии формирования, в то время как криминологическая наука по-прежнему оперирует категориями, выработанными для анализа традиционных, контактных преступлений, где портреты преступника и жертвы были относительно стабильны. Современная цифровая реальность сломала эти стереотипы, требуя фундаментальной переориентации и выработки новых подходов.

Недостаточная изученность данной проблематики напрямую ведет к низкой эффективности профилактической работы. Широко известный факт, что до 95% населения осведомлены о существовании ИТ-мошенничества, но продолжают становиться жертвами, свидетельствует о том, что простого информирования недостаточно. Преступники используют не гипноз, а прицельное воздействие на базовые человеческие эмоции: страх, панику, жадность, а также манипулируют чувством долга и вины. Данные психолого-психиатрических экспертиз, проведенных в рамках расследования уголовных дел, показывают, что потерпевшими чаще становятся лица с определенным психотипом: излишне эмоциональные, тревожные, несамостоятельные в принятии решений, с высоким уровнем долженствования. В свою очередь, социологические исследования (в частности, Центра психологического консультирования НИУ ВШЭ) дополняют этот портрет, указывая, что в группе риска находятся люди с неполным средним и средним образованием, жители сельской местности и граждане, для которых основным источником информации является телевидение.

Таким образом, противодействие дистанционным преступлениям и связанным с ними угрозам требует комплексной, двуединой стратегии. С одной стороны, это усиление правоприменительной практики и совершенствование законодательства. С другой, и это не менее важно, - формирование в обществе «цифрового иммунитета». Эта задача выходит за рамки простой цифровой грамотности и включает в себя развитие навыков критического мышления, самоконтроля и психологической устойчивости к манипулятивным техникам. Чем быстрее научное сообщество, правоохранительные органы и система образования осознают эту необходимость и начнут совместную работу, тем эффективнее мы сможем защитить наших граждан и обеспечить национальную безопасность в новых условиях цифровой эпохи.

Дистанционные преступления и их влияние на террористическую угрозу

Методические материалы

Авторы:

Силантьев Р.А. – профессор кафедры мировой культуры, заведующий лабораторией деструктологии МГЛУ, главный аналитик РАО, доктор ист. наук

Филиппов Д.В. – генерал-майор юстиции, заместитель начальника следственного департамента МВД РФ

Василишина О.М. – полковник юстиции, старший следователь по особо важным делам 2 отдела УвиПК Следственного департамента МВД России

Громова А.Н. – главный специалист методологического отдела Центра психологической безопасности и профилактики деструктивных явлений среди детей и молодежи в Нижегородской области

Тираж 1000 экз. Заказ №14595
Отпечатано в типографии ООО «РИММИНИ»
603104, Нижний Новгород, ул. Краснозвёздная, 7а, оф. 3
Тел/факс: +7(831) 422-57-80 www.rimmini.ru