Волков Геннадий Юрьевич
канд. экон. наук, доцент
ФГКОУ ВО «Ростовский юридический институт МВД России»
г. Ростов-на-Дону, Ростовская область

DOI 10.31483/r-103208

ПРОБЛЕМАТИКА ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСКИМ СХЕМАМ ОБМАНА КЛИЕНТОВ С ИСПОЛЬЗОВАНИЕМ НОВЕЙШИХ МЕТОДИК СОЦИАЛЬНОЙ ИНЖЕНЕРИИ (НА ПРИМЕРЕ ДЕЯТЕЛЬНОСТИ ЗАРУБЕЖНЫХ CALL-ЦЕНТРОВ)

Аннотация*: в статье предпринята попытка анализа основных проблем, связанных с мошенническими действиями работников CALL-центров, расположенных на территории недружественных РФ стран и возможностью минимизации негативных последствий их функционирования для российских клиентов кредитно-финансовых организаций.*

Ключевые слова: *call-центр, противоправная деятельность, конфиденциальная информация, личный кабинет, социальная инженерия.*

Реалии цифровой экономики постиндустриального этапа развития объективно опосредовали появление новейших методов экономико-финансовой деятельности, представляющих собой своего рода «компилят» основных преимуществ, предоставляемых процессов глобализации. Перевод большинства финансовых операций в цифровой сегмент с использованием современных средств коммуникации является объективным продолжением глобализации мирового кредитно-финансового и инвестиционного секторов.

Важнейшим следствием подобной трансформации является осуществление операций в режиме реального времени, возможность оперативной коррекции в соответствии с возникающей необходимостью и скорость выполнения необходимых операций с транснациональными характеристиками.

Возможности современного цифрового пространства позволяют открывать собственные электронные кабинеты пользователя, имеющие достаточную степень защиты от потенциального взлома со стороны мошенников. Однако, как убедительно свидетельствует исторический анализ печального опыта мошеннической деятельности, любые новые веяния в сегменте финансово-экономической деятельности сопровождались противоправными действиями со стороны любителей легкой наживы. В сфере противостояния закона и мошенничества на каждое защитно-блокировочное действие приходилось несколько вариантов его обхода или минимизации конечной результативности.

Одним из наиболее распространенных видов мошенничества последнего времени стала кража персональных данных пользователей, позволяющая злоумышленникам использовать денежные средства или конфиденциальную информацию коммерческого толка. Отличительной особенностью действий мошеннических группировок является принцип «новое – это хорошо забытое старое». В процессах агрессивной атаки на потенциальных «клиентов» из числа мобильных абонентов снова начинают использоваться «отработанные» забытые схемы. Причина крайне проста – учитывая уровень защиты и противодействия используемым методикам, мошенники отказываются от «продвинутых» современных средств противоправных действий, предпочитая возврат к максимально примитивным моделям прошлого. Учитывая тот факт, что большинство клиентов успело забыть о данном методе мошенничества, схема получила широкое распространение с высокой степенью эффективности, особенно среди лиц пожилого возраста.

Принимая во внимание степень охвата клиентов операторами различных структур, наиболее популярной стала схема использования алгоритма «службы клиентской поддержки оператора». К сожалению, достаточно часто соучастником преступных действий на начальном этапе реализации незаконной деятельности являются сами операторы, предоставляющие мошенникам на коммерческой основе данные клиентов, с указанием необходимых параметров.

Причиной прозвона клиента может быть обозначено все что угодно: от смены тарифного плана на более выгодный и заканчивая срочной необходимостью замены имеющейся карты. Цель операции проста: любым способом получить доступ к мобильному кабинету потенциальной жертвы с использованием SMS-подтверждения, поступающего на номер абонента.

Смысл данных действий состоит в том, чтобы, получив доступ к входу в личный кабинет, произвести смену настроек для переадресации SMS и звонков с номера потенциальной жертвы на номер мошенника, что позволит получать все аутентификационные сообщения для необходимого подтверждения разного рода операций. В числе приоритетных встречаются вывод средств с карты клиента и незаконное оформление кредита на собственника кабинета. «Высшим достижением» подобных схем является принуждение абонента самостоятельно выполнить операцию по подключению «шпионской услуги» переадресации вызовов или SMS со своих активно используемых мобильных устройств. В процессе разработанной с учетом психологических методик беседы с клиентом, мошенники просят самостоятельно набрать USSD-команду и номер, на который будут перенаправлены звонки и сообщения

Сразу необходимо особо подчеркнуть, что в случае возникновения подобной ситуации, необходимо постоянно помнить, что представители оператора связи не имеют права на запрос кода и любой информации, которая носит конфиденциальный характер для доступа в личный кабинет. При малейшем подозрении или сомнении в действиях оператора, необходимо незамедлительно прервать диалог, после чего оперативно связаться со службой поддержки оператора или (и) проверить информацию по предоставляемой услуге на сайте оператора.

Как правило, в алгоритме действия любого оператора по предоставлению услуг, используется постоянно совершенствующаяся модель защиты, которая в приоритетном порядке блокирует возможность переадресации SMS-сообщения с кодами подтверждений от банков. Подверглась детальной доработке «антифродовая система», которая позволяет блокировать подобные действия. в режиме

реального времени с одновременным отслеживанием любых подозрительных звонков для максимально оперативной блокировки.

Однако не стоит забывать, что современный преступный мир ориентируется, в первую очередь на привлечение квалифицированных специалистов, деятельность которых позволяет обходить используемые системы защитных мер.

Согласно оперативным отчетам, предоставленных аналитиками «Лаборатории Касперского», использующих данные приложения «Kaspersky Who Calls» и МВД, по итогам 2021 г. сумма совокупного объема ущерба от телефонного мошенничества в РФ составила минимум 45 млрд рублей. При этом среднестатистический показатель суммы ущерба для одного инцидента варьируется от 15 тыс. рублей до десятков миллионов, а зафиксированный максимум составил 25 млн рублей.

Анализ предоставленных данных позволяет говорить о дальнейшем росте числа рассматриваемых противоправных действий в первом квартале 2022 г., поскольку доля российских пользователей, получивших звонки подобного рода, достигла 4,9% от общего числа звонков.

Особую проблему для правоохранительных структур представляло то обстоятельство, что большинство звонков поступало с территории Украины. Начало военной спецоперации к демилитаризации и денацификации Украины позволило уничтожить ряд системы call-центров, расположенных на территории Днепропетровска, откуда поступала большая часть звонков. Было зафиксировано частичное временное снижение активности, вызванное необходимостью обустройства новых центров, набором персонала и его обучения.

К сожалению, организация деятельности подобного рода относится к категории «малозатратной», поскольку основу деятельности составляет аренда минимальной площади, крайне бюджетный набор IP-телефонии и минимальный штат, способный выполнять примитивные операции.

В подтверждение данного вывода можно привести возобновление деятельности криминальных call-центров, сотрудники которых после непродолжительного периода, связанного с необходимостью перегруппировки и максимальной

адаптации к сложившимся реалиям, обрушили на пользователей новый вал «токсичных звонков».

Особую тревогу у правоохранителей вызывает тот факт, что успехи российской армии вызывают крайне негативную реакцию у представителей националистической прослойки украинского населения, особенно из западных областей, что объективно способствует увеличению объемов подобной деятельности. Более того, учитывая тренд формирования антироссийских настроений, география создания call-центров, с ярко выраженной антироссийской составляющей, стремительно расширяется, перемещаясь на территорию Польши, Румынии, Венгрии, Чехии и других недружественных государств [2, с. 81].

В процессах структуризации противоправной деятельности, активно используются беженцы и переселенцы, а также представители местного населения с открыто выраженными русофобскими настроениями. Учитывая проблемы с трудоустройством и выплатой денежных пособий, правительства обозначенных стран проявляют определённую заинтересованность в развитии противоправной деятельности.

В этой ситуации была оперативно разработана новая схема: блокировка счета в связи с переводом денежных средств в недружественное государство, прежде всего на Украину, который специалист call-центра позиционирует в разговоре как факт поддержки противника.

В данном случае мошенники используют двойную схему обмана для граждан обоих государств. К традиционной мантре о потери денег, добавляется в качестве усиливающего фактора давления возможность дифференциации перевода в качестве финансовой поддержки ВСУ. Кроме того, в качестве нового способа психологического давления используется убеждение клиента в том, что, он участвует в спецоперации органов и обязан все свои действия сохранять в строжайшей тайне. К сожалению, для большинства пожилых и впечатлительных клиентов, данная методика продемонстрировала максимальную эффективность.

В случае «запуска процесса» используется ранее обозначенный алгоритм: «сотрудник банка» получает персональную информацию, после чего деньги уходят на счет, подконтрольный преступникам. Если клиент отказывается от разговора, через определенный временной интервал поступает новый звонок, в процессе которого бот сообщает, что счет заблокирован в связи с упомянутой причиной, после чего начинается активное психологическое давление, целью которого является произнесение клиентом слова «*да*», после чего разговор моментально переводится на «живого» оператора, который продолжает активную атаку с использованием новейших методов социальной инженерии [3, с. 437].

По мнению большинства аналитиков, занимающихся проблемами минимизации негативных последствий деятельности мошенников, алгоритм структурирования мошеннических схем несет цикличный характер, что позволяет просчитать вероятность повторного использования ранее применяемых моделей [1, с.7]. С другой стороны, существует реальная возможность подготовить комплексную защиту с учетом коррекционных мер, обусловленных изменением макроэкономической ситуации. В среднем, цикл сменяемости используемых походов составляет от 6 до 12 месяцев, в зависимости от направления и объемов перспективной деятельности преступников.

Самые большие опасения у правоохранительных структур вызывают темпы глобализации мировой преступности и перевода противоправных действий с регионального через национальный на транснациональный уровень. При этом преступления в сегменте электронной коммерции трансформируются в неотъемлемый элемент современной противозаконной деятельности.

В процессах адаптации социотехнических схем противоправной деятельности мошенники все чаще начинают использовать реалии санкционного противостояния, политику «зеркального ответа» и т. д. В частности, резкое увеличение числа нежелательных звонков от злоумышленников все чаще обуславливается технологическим саботажем владельцев серверов, на которых хранятся базы приложений по распознаванию и блокировке нежелательных звонков.

Пользователь, который систематически подвергается спам-атакам и звонкам мошенников, старается установить дополнительное число приложений и использовать все возможности расширения браузера, что позволяет использовать вариативную модель блокировки и защиты. Но для работы практически всех доступных на территории РФ программ и пакетных решений необходим доступ к базам, которые хранятся на серверах недружественных стран, активно проводящих русофобскую политику.

С одной стороны, после февраля 2022 г. приложения продолжают работать, но при этом, большинства баз для пользователей из РФ не предполагает необходимой процедуры обновления. С другой стороны, этот же процесс работает и в обратном направлении, т.е. базы большинства из них не обновляются данными от российских пользователей. Данный процесс сознательно отключен владельцем сервера, что приводит к тому, что процесс блокировки не активирован, база не обновляется, а весь объем нежелательных звонков беспрепятственно доходит до клиента.

В этой связи, для минимизации негативных последствий от действий мошенников, необходимо помимо чисто технических моментов, учитывать следующие:

– отделам безопасности банковского сектора и операторам связи необходимо находиться в постоянном контакте с разработчиками систем защиты для постоянного обновления имеющихся защитно-блокировочных программных пакетов;

– активнее использовать возможности крипто-шифрования и усиленной цифровой подписи при структурировании процессов кредитно-финансовой деятельности;

– принимая во внимание тот факт, что основным инструментом злоумышленников является использование новейших приемов и методов социальной инженерии, провоцирующих ситуацию психологического прессинга, в результате чего осуществляется добровольное сообщение требуемых данных, при малейшем подозрении необходимо немедленно прекратить разговор;

– поскольку, находясь под воздействием психологического давления субъект осуществляет перевод денежных средств или сообщает банковскую информацию, в рамках действующего законодательства, банки не обязаны компенсировать похищенную сумму. В этом случае, также необходимо немедленное прекращение словесного контакта, после чего следует проинформировать отдел безопасности банка о попытке мошенничества.

В ситуации, когда в составе семьи имеется родственники преклонного возраста или люди со сниженным уровнем адекватного реагирования, необходимо максимально ограничить возможность вовлечения их в диалог с мошенниками.

Достичь оптимального баланса в процессах защиты денежных средств и конфиденциальной информации можно только при использовании всего арсенала защитных средств заинтересованных организаций и максимального внимания к заблаговременному построению поведенческих моделей индивида в рассмотренных ситуациях.

Список литературы

1. Седойкина А.А. Перспективы внедрения системы искусственного интеллекта для повышения эффективности бизнес-процессов в call-центре / А.А. Седойкина // Human Progress. – 2020. – Т. 6. №2. – С. 7. – DOI 10.34709/IM.162.7. – EDN OMRIDB.

2. Шилкин Л.А. Оценка психологических важных показателей оператора call-центра / Л.А. Шилкин // Социально-гуманитарные технологии. – 2020. – №3 (15). – С. 80–87. – EDN HRFMMJ.

3. Щербакова Е.Г. Оценка эффективности взаимоотношений банка с клиентами с использованием телекоммуникационных технологий call-центра / Е.Г. Щербакова // Финансовая экономика. – 2018. – №4. – С. 435–439. – EDN RXLKPJ.