Анализ мошеннических звонков с территории Украины

Участники и цифры

Ноябрь 2022

Содержание

Введение 2
1. Мошеннические SIP-сервисы 3
2. Операторы, участвующие в пропуске мошеннического трафика 5
3. Скрипты мошеннических диалогов 8
4. «Рейтинг» операторов сотовой связи 9
5. Телефонное мошенничество – меры противодействия 10
Заключение 12

Введение

За последние несколько лет на территории России наблюдается рост количества дистанционных преступлений – телефонного мошенничества, которое реализуется методами социальной инженерии. Так, по данным Банка России[1],во II квартале 2022 года граждане РФ под воздействием третьих лиц перевели злоумышленникам денежные средства 211 тыс. раз, общая сумма составила 2,8 млрд руб. Реальная картина финансовых потерь превышает статистику Банка России в разы – объем мошенничества в РФ оценивается суммами от 55 (оценка МВД) до 150 млрд рублей (оценка экспертов) в год. По данным Сбера, на социальную инженерию приходится 90% всех финансовых преступлений, из них 94% — это телефонное мошенничество[2].

Ранее эксперты считали, что количество звонков из мошеннических call-центров составляет до 100 тыс. в сутки. Однако в 2022 г. Сбер завершил проект по подключению антифрод-систем основных операторов сотовой связи к своей системе транзакционного антифрода, что позволило увидеть полную картину по мошенническим звонкам. Так, по оценке Сбера, в 2022 году мошенники сделали 1,5 млрд попыток позвонить клиентам банков с целью похищения денежных средств. В течение последнего полугодия только в Сбере такие попытки затронули более 65% клиентов. В день совершается около 5 млн звонков, в том числе, с помощью роботизированных виртуальных ассистентов. Через форму обратной связи в мобильном приложении СберБанк Онлайн клиенты пожаловались на 1,8 млн телефонных звонков от мошенников.

В результате взаимодействия с правоохранительными органами в рамках расследования деятельности call-центра в г. Бердянск было установлено, что подавляющее большинство звонков поступает гражданам России, на втором месте – граждане Польши. Ранее на третьем месте была Германия, но в июле 2022 г. звонки в эту страну прекратились, после чего в топ стран вошли Казахстан, Таджикистан и Беларусь.

По нашей оценке, многолетний тренд роста телефонного мошенничества сохранял актуальность вплоть до февраля 2022 года. В январе клиенты Сбера 250 тыс. раз пожаловались в банк на мошенничество, в феврале было зафиксировано 264 тыс. обращений – на 6% больше. После 24 февраля 2022 года была зафиксирована полная остановка «мошеннического конвейера». Через месяц начался плавный рост, но количество жалоб снизилось в 5,5 раз[3] (с 11 тыс. до 2 тыс. в сутки).

По экспертной оценке Сбера, до 90% call-центров, работающих против граждан РФ, находятся на территории Украины, остальные располагаются в России и странах СНГ.

[1] Отчет Банка России за 2 квартал 2022 г. – http://www.cbr.ru/analytics/ib/review_2q_2022/

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

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

Общий объем похищенных украинскими call-центрами средств достигал 75 млрд руб. в 2020 г. В ноябре 2022 г. количество звонков из украинских call-центров составляло только 70% от наблюдаемого в начале года. По нашей оценке, причины этого падения связаны с ликвидацией действующих call-центров и проводимой профильными ФОИВ[4] и операторами связи работой по наведению порядка в телефонии.

Ранее в отчете раскрывались детали работы одного из мошеннических call-центров в г. Бердянске. Информация о сотрудниках, их роли и используемые инструменты позволили правоохранительным органам установить личности всех злоумышленников и объявить их в розыск.

В данном отчете эксперты Сбера исследуют тему мошеннических звонков, анализируют известные мошеннические SIP[5]-сервисы, статистику звонков, рассматривают их сценарии, а также предлагают комплекс мер по противодействию.

1. Мошеннические SIP-сервисы

В рамках расследования деятельности call-центра в г. Бердянск экспертам Сбера удалось идентифицировать SIP-серверы, через которые совершались мошеннические звонки гражданам РФ и других государств. Было установлено, что данные сервисы активно используются и в других call-центрах, действующих на территории Украины. Всего было выявлено более 50 таких серверов. Вот некоторые из них:

- dids.phonet-tel.com (Германия);
- spgsipt2.xyz (Германия);
- spgsip.com (Голландия);
- sip.freevoip.org (США);
- sip2.voipex.top (Германия);
- sr1.phonet-tel.com (Германия).

Общее количество мошеннических звонков, прошедших через данные сервисы за два последних года, превысило **37 млн**. При этом звонки осуществлялись с подстановкой нумерации московского региона 495/499, что является нарушением требований действующего ФЗ «О Связи» (запрещены звонки с российских номеров из-за границы). Большая часть звонков нацелена на лиц, проживающих на территории РФ, однако мошенники звонят и жителям других стран.

Отдельно необходимо отметить, что не зафиксировано фактов обзвона граждан Украины, находящихся на ее территории. Таким образом, подтверждается отмеченное нами в предыдущем отчете соблюдение принципа не воровать у граждан Украины.

[4] https://ru.wikipedia.org/wiki/%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5_%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D1%8B_%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D0%BD%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9_%D0%B2%D0%BB%D0%B0%D1%81%D1%82%D0%B8

[5] https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%83%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D1%81%D0%B5%D0%B0%D0%BD%D1%81%D0%B0

В результате анализа журналов звонков с 14.12.2021 г. установлено ведение целенаправленной мошеннической активности против граждан различных стран. Приведем основные цифры:

- Польша – 380 тыс. звонков;
- Казахстан – 36 тыс. звонков;
- Таджикистан – 18 тыс. звонков;
- Грузия – более 8 тыс. звонков;
- Кыргызстан – 8 тыс. звонков;
- Узбекистан – 7,5 тыс. звонков.

Звонки осуществляются в основном русскоговорящим клиентам. Однако мошенники общаются и с гражданами Польши на польском языке (подробнее – в разделе 3). При этом основной сценарий обмана – звонок от имени службы безопасности банка с зафиксированной заявкой на смену «финансового номера телефона».

Далеко не все попытки мошенников позвонить оказываются успешными. Лишь 0,1% клиентов ведут со злоумышленниками длительную беседу (более 10 мин.). Стоит отметить, что в выходные дни, когда у клиентов есть больше времени, повышается средняя продолжительность диалога с мошенниками.

В начале 2022 года наблюдался самый высокий показатель средней длительности диалога клиентов с мошенниками – 1 минута, в марте произошло снижение до 50 секунд (на 16%). Затем этот показатель сократился до 40 секунд.

Режим работы сотрудников call-центров – обычно с 9 до 18 ч., реже с 8 до 17 ч. (по украинскому времени). Обзвоны проводятся по будням, 1-2 раза в месяц в call-центрах бывают «рабочие субботы». Иногда звонки совершаются и в воскресенье либо в ночное время (клиентам с Дальнего Востока).

2. Операторы, участвующие в пропуске мошеннического трафика

Для выявления операторов, участвующих в пропуске мошеннического трафика на территорию РФ, эксперты Сбера совместно с правоохранительными органами сделали контрольные закупки услуг с подменой номера через указанные сервисы SIP-телефонии. В результате был получен список операторов (см. таблицу 1). Правоохранительные органы ведут работу с ними, поэтому часть данных скрыта.

А-номер	Оператор	ИНН	Веб-сайт
7[redacted]6	ООО "[redacted]"	[redacted]3	https://[redacted].com/
7[redacted]4	АО "[redacted]"	[redacted]3	https://www.[redacted].ru/
7[redacted]4	АО "[redacted]"	[redacted]5	https://www.[redacted].ru/
7[redacted]8	АО "[redacted]"	[redacted]3	https://www.[redacted].ru/
7[redacted]9	ООО "[redacted]"	[redacted]5	https://[redacted].ru/
7[redacted]4	ООО "[redacted]"	[redacted]4	https://www.[redacted].ru/
7[redacted]2	АО "[redacted]"	[redacted]3	https://www.[redacted].ru/
7[redacted]8	ООО "[redacted]"	[redacted]1	https://[redacted].com/
7[redacted]2	ООО "[redacted]"	[redacted]0	http://www.[redacted].ru/
7[redacted]8	ООО "[redacted]"	[redacted]1	https://[redacted].com/
7[redacted]6	ООО "[redacted]"	[redacted]5	https://[redacted].ru/
7[redacted]2	ООО "[redacted]"	[redacted]4	https://www.[redacted].ru/
7[redacted]2	ООО "[redacted]"	[redacted]1	https://[redacted].com/
7[redacted]7	АО "[redacted]"	[redacted]3	https://www.[redacted].ru/
7[redacted]8	ООО "[redacted]"	[redacted]1	https://[redacted].com/

Таблица 1. Перечень операторов, участвующих в пропуске мошеннического трафика

В интернете можно найти множество отзывов обычных граждан о мошеннических звонках, совершенных через данных операторов.

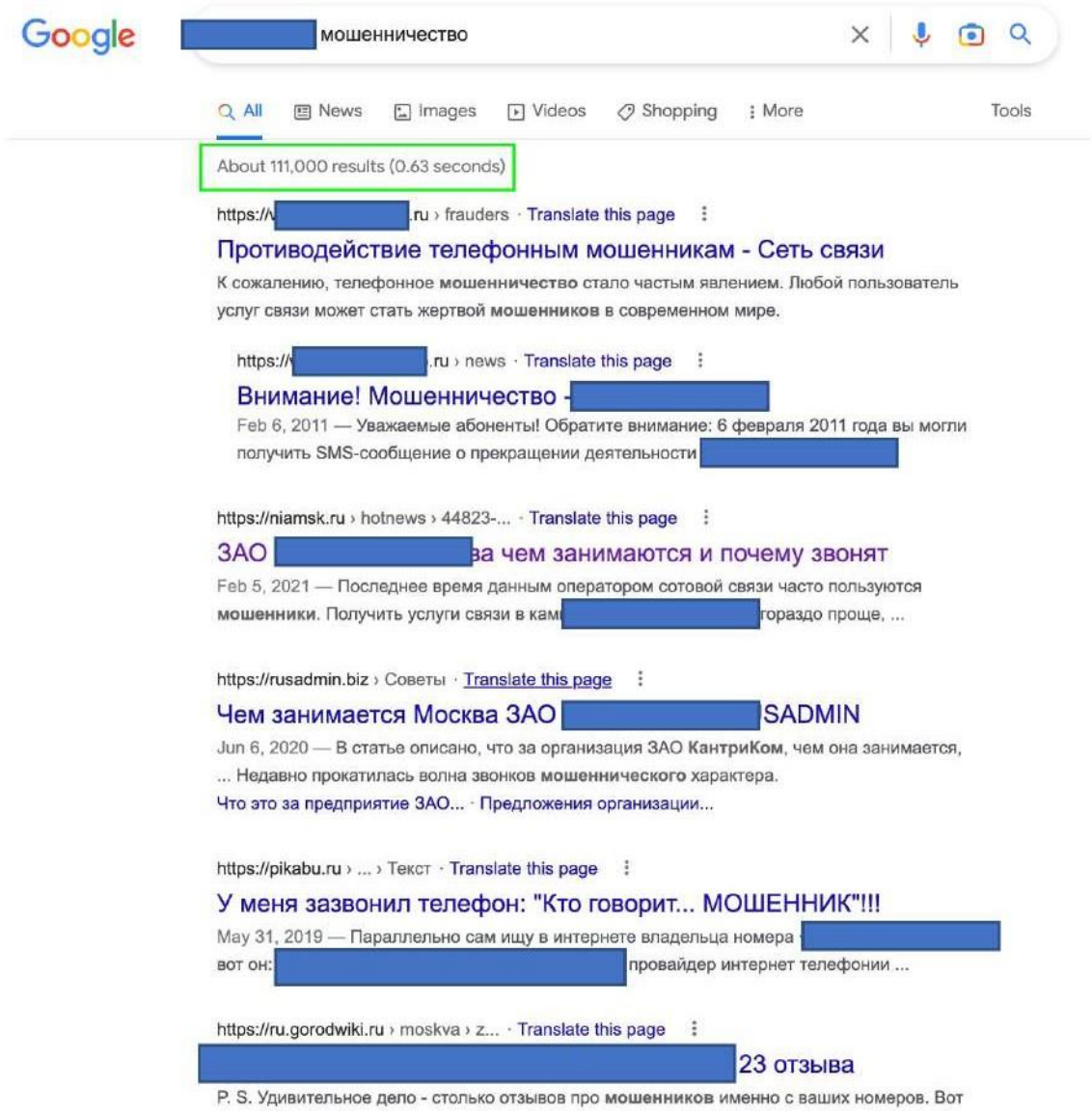

Рисунок 1. Пример отзывов на мошеннические звонки от одного из выявленных операторов

Таким образом, выявлены многочисленные факты нарушения операторами действующего ФЗ «О связи». За это предусмотрен, как минимум, административный штраф.

Рассматривая список используемых для мошеннических звонков SIP-сервисов, отметим, что большинство из них расположены в Германии и Франции. Однако можно выделить и русскоязычный сервис mithuntele.com – «BLACK VOIP. Звонки с подменой номера по всему миру без ограничений». В описании указано, что он создан для совершения полукриминальных или криминальных звонков.

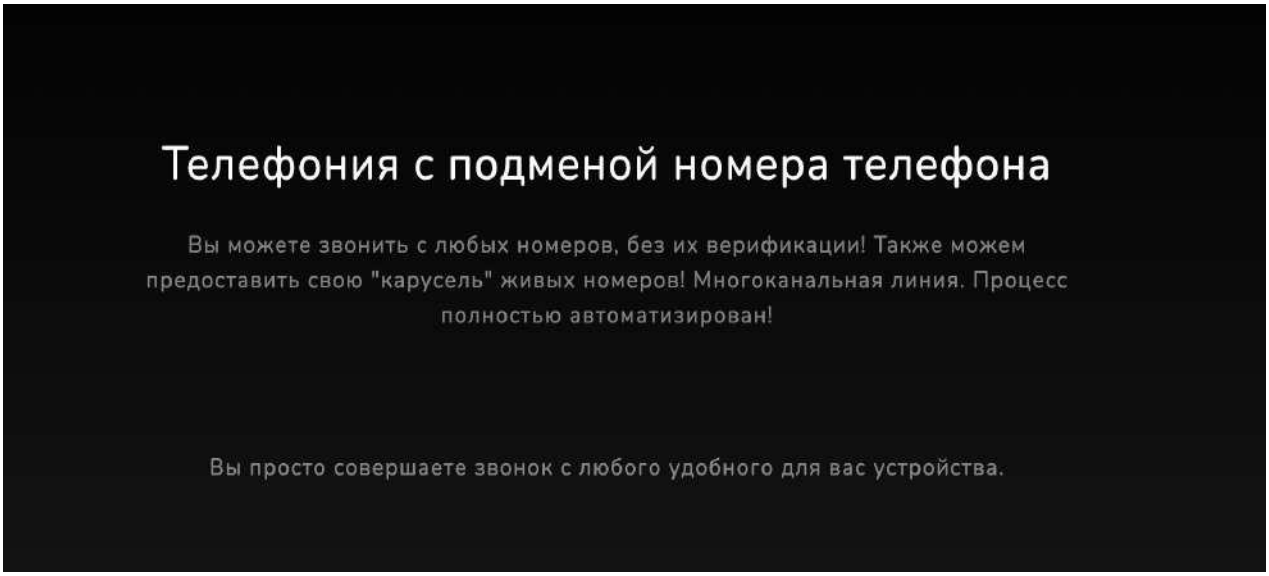

Рисунок 2. Приветственный экран SIP-сервиса mithuntele.com

При анализе данного ресурса был установлен контакт его владельца. Анализ активности этого человека в Телеграмм-каналах показывают, что он активно интересуется объектами недвижимости Украины (Днепр, Одесса) и РФ (Москва и Московская область), торговлей украденными базами данных, работой в теневом сегменте интернета. Вся собранная по данному лицу информация передана в правоохранительные органы для проведения оперативных мероприятий.

Также в рамках исследования деятельности украинских call-центров нами установлено, что злоумышленники организовали локальные филиалы своего центра в различных регионах Украины (Днепр, Одесса, Запорожье и т.д.). Всего было обнаружено более 40 таких филиалов. Организация телефонии в них велась через специально разработанное программное обеспечение на базе OpenSource ПО OSDial[6].

Рисунок 3. Пример входа в интерфейс ПО OSDial

[6] https://osdial.com/

Установлено, что разработчики ПО участвовали в настройке и организации работы данного call-центра. Вся собранная экспертами Сбера информация передана сотрудникам полиции.

3. Скрипты мошеннических диалогов

Экспертами Сбера проведен анализ типовых сценариев обмана в разных странах. Результаты представлены в таблице ниже.

Страна	Сценарий	Организация, от имени которой осуществляется звонок	Язык общения	Сценарий обмана
РФ	Смена финансового номера	Банки РФ	Русский	Жертве поступает звонок якобы от имени банка с целью подтверждения смены финансового номера. Если жертва отрицает наличие такового номера, мошенник сообщает, что с ней свяжутся из полиции для расследования неправомерных действий. Далее звонок передается на «вторую линию»[7], где жертву вынуждают совершить операции в рамках «специального полицейского расследования».
РФ	Оформление кредита	Банки РФ	Русский	Жертве поступает звонок якобы от имени банка с сообщением, что на ее имя оформляется кредит. Если жертва отрицает запрос кредита, ей сообщают, что необходимо подать заявку на новый кредит через мобильное приложение банка, а банк самостоятельно отменит текущую заявку. После зачисления кредита от банка мошенники убеждают жертву перевести средства на «безопасный счет», т.к. счет клиента был скомпрометирован.

[7] Подробней о первой и второй линии см. «Отчет о расследовании деятельности мошеннического call-центра в г. Бердянск».

Польша	Оформление кредита	PKO Bank Polski SA[8]	Польский	Мошенник звонит клиенту с целью подтверждения зачисления оформленного кредита. После сообщения клиента о том, что он не оформлял кредит мошенник фиксирует информацию и «передает в ПХО». Просит ожидать звонка от ПХО. Далее сценарий аналогичен сценарию 1 для РФ.
Казахстан	Попал в ДТП	-	Русский	Мошенник под видом потерпевшего звонит родственнику и сообщает, что попал в ДТП и ему нужна помощь.
Германия	Смена финансового номера	Sparkassa bank	Русский	Аналогичен сценарию 1.

Таблица 2. Результаты анализа сценариев звонков в разные страны из мошеннического call-центра Украины

Таким образом, основные сценарии обмана не сильно отличаются от уже отработанных на гражданах РФ. При этом звонки в Германию осуществляются по списку русскоязычных граждан. Если они сообщают, что прибыли в Германию в качестве беженца и являются гражданами Украины, – сценарий обмана прерывается и жертву инструктируют, как следует вести себя при аналогичных звонках.

Также из особенностей необходимо выделить схему «родственник в беде» (Казахстан). Данная схема ранее активно применялась против граждан РФ call-центрами, действующими в учреждениях ФСИН.

4. «Рейтинг» операторов сотовой связи

Операторы связи ведут работу по противодействию токсичным звонкам (СПАМ, операторский фрод, мошеннические звонки с использованием методов социальной инженерии). Детали этой деятельности нам не известны. Однако Сбер, агрегируя информацию о жалобах на попытки обмана, анализирует эти данные и на их основе делает выводы об эффективности противодействия.

[8] https://ru.wikipedia.org/wiki/PKO_Bank_Polski

Рисунок 4. Доли операторов связи по количеству полученных мошеннических звонков

В набольшей степени от телефонного мошенничества защищены абоненты МТС.

5. Телефонное мошенничество – меры противодействия

Техническим решением проблемы могла бы стать система верификации вызовов. По требованиям ФЗ «О Связи», с января 2023 г. она должна быть обязательной для операторов. Однако пока система не создана, соответственно, невозможно оценить ее эффективность.

Кроме того, необходимо учитывать, что после создания данной системы для ее обхода мошенники наверняка изменят схемы обзвона (например, перейдут в мессенджеры или будут использовать звонки без подмены номеров). Поэтому одновременно с внедрением системы потребуется активнее наказывать операторов связи за нарушение законодательных требований.

Несмотря на закрепление в ФЗ «О связи» определенных обязанностей операторов связи, длительное время никакой ответственности за их неисполнение не было. Только с начала 2022 года появилась возможность привлечения операторов к административной ответственности за пропуск из-за границы звонков с российскими номерами, за подмену номера абонента и

другие нарушения закона «О связи».

Более 30 операторов, из-за неправомерных действий которых стало возможным совершение преступлений, были привлечены к административной ответственности. Некоторые из них – неоднократно. В то же время, несовершенство законодательства о связи, отсутствие иных рычагов влияния на недобросовестных операторов не позволяет правоохранительным органам эффективно бороться с ИТ-преступностью.

Основными проблемами и способами их решениями являются:

1. Простота получения лицензий и доступа на рынок услуг связи. Чтобы не допустить в эту сферу недобросовестных игроков, необходимо упростить порядок аннулирования лицензии, предоставив право на обращение в суд в том числе органам прокуратуры, а также возможность внесудебного решения вопроса лицензирующим органом в случае неоднократного нарушения оператором связи требований законодательства.

2. Подавляющее большинство звонков с подменными номерами приходит по VOIP-сетям и переводится операторами в телефонные сети. Однако порядок присоединения VOIP-сетей к телефонным сетям не урегулирован. Запрет на передачу IP-вызова из сети передачи данных в телефонную сеть в законодательстве отсутствует. Операторы, руководствуясь принципом «все, что не запрещено – разрешено», переводят такие вызовы. Для исключения такой возможности и установления ответственности операторов необходимо на уровне ФЗ закрепить запрет на перевод вызова из VOIP-сетей в телефонные сети, либо необходимость урегулирования порядка присоединения этих сетей связи. Одновременно с л е д у е т предусмотреть административную ответственность за неисполнение указанных норм.

3. В случае совершения преступления правоохранительным органам важно в кратчайший срок установить источник поступления звонка. Поэтому от операторов требуется предоставление сведений либо о факте инициирования звонка его абонентом, либо об операторе, от которого им поступил вызов. Однако это сделать не удается из-за длительной процедуры установления всей цепочки передачи трафика и определения первого оператора, пропустившего «криминальный» звонок, а также из-за неготовности операторов связи предоставлять информацию без судебного решения.

Для устранения неопределенности и законодательного закрепления обязанности операторов связи предоставлять такую информацию по запросам уполномоченных органов без судебного решения и в ограниченный срок необходимо внести соответствующие дополнения в ФЗ «О связи». Одновременно следует предусмотреть административную ответственность за неисполнение данной обязанности.

Операторов связи, пропускающих «теневой» трафик, порой не останавливает возможность привлечения к ответственности по статье 13.2.1

КоАП РФ за передачу измененного номера и непрекращение оказания услуг. Их дневные доходы от незаконной деятельности многократно превышают штрафные санкции (от 30 тыс. до 1 млн руб.).

В УК РФ отсутствует норма, позволяющая привлечь работников оператора связи к уголовной ответственности за такие действия. Доказать факт соучастия в конкретном преступлении, а также умысел практически невозможно.

В этой связи предлагается установить уголовную ответственность работников операторов связи за неоднократное нарушение закона о связи, повлекшее причинение существенного вреда правам и законным интересам граждан (организаций) либо интересам общества или государства.

Реализация мер позволит не только эффективно применять штрафные санкции к «серым» операторам, но и привлекать их работников к уголовной ответственности, лишать лицензий организации, систематически нарушающие закон. В итоге это должно способствовать уходу с рынка недобросовестных игроков, являющихся звеньями в преступной схеме.

Заключение

Большинство преступлений совершено при помощи средств телефонной связи посредством подмены абонентских номеров. Наиболее ярко изменения в структуре преступности проявляются в Москве, где киберпреступления составляют почти 40 % от всех зарегистрированных посягательств.

Для введения граждан в заблуждение злоумышленники используют телефонные номера московского региона, кредитных организаций, органов государственной власти и правоохранительных структур.

Подмена абонентских номеров используется также для совершения действий экстремистского и террористического характера, незаконного оборота наркотиков и других противоправных действий. Значительная часть звонков осуществляется с территории других государств, преимущественно из Украины.

По мнению экспертов, отдельные действия операторов связи на территории России могут быть расценены минимум как недружественные, что должно иметь самую жесткую оценку со стороны правоохранительных органов.

Вместе с тем, простота реализации массовых звонков через IP-телефонию, высокий уровень зрелости ИТ-инфраструктуры для поддержки данных звонков требуют адекватных и эффективных мер противодействия. Они сформулированы и должны быть реализованы на государственном уровне.