Интервью начальника управления по надзору за уголовно-процессуальной и оперативно-разыскной деятельностью прокуратуры республики

Сергеева Ивана Анатольевича

Иван Анатольевич, расскажите пожалуйста о данных по количеству пострадавших от действий дистанционных мошенников и какова сумма ущерба, нанесенного гражданам республики за 2025 год?

Добрый день! В последние годы фиксируется постоянный рост преступлений, совершенных с использованием информационно-телекоммуникационных технологий, в том числе корыстной направленности. Жители страны, и уже не только пожилого возраста, становятся жертвами телефонных мошенников.

В 2025 году в республике зарегистрировано 6402 преступления в сфере ИТТ (2024 год – 4588; + 39,5%). Удельный вес таких преступлений составил 43,6% от общего количества всех зарегистрированных в регионе преступлений.

Почти половину об общего числе киберпреступлений составили дистанционные хищения денежных средств граждан, включая кражи и мошенничества (46%).

Жертвами мобильных мошенников стали свыше 2,2 тысю жителей республики (2024 год – 2,6 тыс.). Размер причиненного им ущерба превысил 835 млн рублей (2024 год - 1,1 млрд. руб.).

Наибольшее количество таких преступлений, как правило, совершается в крупных городах и районах республики – это города Якутск, Нерюнгри, Мирный, Алданский, Ленский, Мегино-Кангаласский и Хангаласский районы.

Превалирующими возрастными группами населения, в отношении которых совершены преступления, оказались граждане от 30 до 49 лет (38,7%), от 60 и старше (21,5%), от 18 до 24 (15,6%), от 50 до 54 (9,9%), от 55 до 59 (7,2%), от 25 до 29 (7,1%).

Социальный статус потерпевших характеризуется следующим образом: работающие по найму – 41,8%; пенсионеры – 15,1%; лица без постоянного источника дохода – 21,7%; государственные и муниципальные служащие – 9,9%; студенты – 6,5%; субъекты предпринимательской деятельности – 1,2%, иные – 3,8%.

Таким образом, потерпевшими от таких преступлений становятся не только излишне доверчивые граждане преклонного возраста, но и молодые люди с высшим образованием, имеющие постоянное место работы (учителя, преподаватели, медицинские и социальные работники, работники органов местного самоуправления, органов государственной власти, крупных промышленных предприятий и т.д.). При этом, большинство потерпевших владели сведениями из средств массовой информации об имеющихся фактах дистанционного мошенничества, но не знали в точности о способах совершения обмана.

Изменились ли способы и схемы хищений, которые применяют мошенники?

Да, способы дистанционных мошенничеств постоянно меняются и адаптируются. Мошенники используют новые технологии и методы, чтобы обмануть людей. Анализ складывающейся в республике криминогенной обстановки свидетельствует о том, что наиболее распространенными способами совершения

дистанционных хищений на сегодняшний день являются:

- «**участие в специальной операции**». Потерпевшим сообщают о некой проблеме, якобы злоумышленники в соучастии с работниками банка оформляют несанкционированный кредит и с целью предотвращения этих действий предлагается оформить встречный кредит, а полученные деньги перевести на так называемый «безопасный счет» либо «специальную ячейку». Одним из способов вовлечения потерпевшего в комбинацию является поступление звонков от лжесотрудников правоохранительных органов (ФСБ, МВД), Росфинмониторинга, Центрального банка России. Для достоверности они могут отправить фотографию поддельного удостоверения, а также различных бланков официальных органов.

- поступление звонков от лжесотрудников операторов сотовой связи с сообщением об окончании срока обслуживания сим-карты.

Потенциальной жертве звонят и представляются работниками операторов сотовой связи, сообщают, что заканчивается срок обслуживания сим-карты, и в целях избежания её блокировки необходимо продлить срок обслуживания путем сообщения «оператору» поступающих на сотовый телефон кодов. В действительности, поступающие коды являются способом для входа в учетную запись потенциальной жертвы на портале «Госуслуг».

- **поступление звонков или сообщений «от имени руководителя»: мошенники выдают себя за директора, главврача, ректора университета и других руководителей организаций, предприятий, в которых работают или работали граждане.**

Например, мошенники совершают звонок от имени начальника, в других случаях подделывают аккаунт руководителя в социальных сетях и предупреждают, что сейчас позвонит сотрудник полиции, ФСБ или Центробанка по очень важному вопросу. После чего поступают звонки от лжесотрудников органов правоохраны или банков о якобы подозрительных операциях по банковским счетам и в целях их предотвращения необходимо следовать их инструкциям о переводе средств на безопасные счета. Весьма часто, мошенники сообщают о том, что со счета потерпевшего идет финансирование вооруженных сил Украины. Также предупреждают о том, что разговор между ними и гражданином является строго конфиденциальным и запрещают об этом кому-либо рассказывать, в том числе близким родственникам, сотрудникам органов правоохраны или банков. В результате чего доверчивые люди становятся жертвой мошенников.

Другой наиболее распространенный способ - это мошенничество с инвестициями в ценные бумаги и криптовалюту.

В этом случае мошенники, пользуясь желанием потерпевшего получить «легкие» деньги, заставляют его инвестировать денежные средства в приобретение криптовалюты, а также различных акций. Далее следует схема по выманиванию денег на различные расходы, связанные с получением лицензии, оформлением страховки и т.д. Как правило, для придания правомерности своим действиям, они позволяют потерпевшим снимать некоторую часть денег, но это не более 10 тыс. руб.

Приведите, пожалуйста, примеры уголовных дел, которые возбуждаются гораздо чаще в настоящее время?

В последнее время мошенники очень активно начали действовать от имени работников операторов сотовой связи, ресурсоснабжающих организаций (Энергосбыт, Водоканал), Пенсионного фонда, налоговых органов, поликлиники под различными

предлогами, такими как необходимость продления срока сим-карты, замена счетчиков (электроприборов), перерасчет пенсии, наличие налоговой задолженности, запись к врачу. В ходе общения мошенники предлагают оформить заявку по телефону, требуя сообщения им кода (якобы номера заявки, очереди), поступившего на телефон потенциальной жертвы. После сообщения данного кода следует звонок от лжесотрудника Госуслуг о взломе личного кабинета на портале, о нахождении денег в опасности, необходимости дальнейшего разговора с сотрудником Росфинмониторинга, Центробанка, МВД и ФСБ, и далее следует стандартная схема по направлению денег на «безопасный» счет.

Например, в мае 2025 года мошенники под видом звонка работника Энергобыта о необходимости замены приборов учета похитили у семейной пары более 24 млн. руб. По данному факту следователями возбуждено уголовное дело. По результатам проведенных оперативно-розыскных мероприятий на территории Томской области установлены лица, причастные к совершению преступления. В настоящее время расследование уголовного дела продолжается.

Стоит отметить, что мошенники общались с данной семьей целый месяц, при этом звонили по видеосвязи, показывали служебные удостоверения и различные официальные бланки.

Что вы можете порекомендовать, чтобы уберечься от таких преступлений и не стать жертвой злоумышленников?

Чтобы уберечься от таких преступлений и не стать жертвой злоумышленников нужно помнить, что в телефонных разговорах мошенники могут выдавать себя за сотрудников Центрального банка, правоохранительных органов (МВД, ФСБ, прокуратуры), за сотрудников ресурсоснабжающих организаций (Энергосбыта, Водоканала) и других учреждений (поликлиник, пенсионного фонда, Росфинмониторинга, ГАВСА). Не надо верить! Нужно помнить, сотрудники ФСБ, МВД, прокуратуры и Центрального банка никогда не проводят какие-либо операции по предотвращению потери денег через телефон, не просят перевода денег на счета третьих лиц.

Также надо помнить, что сотрудники официальных ведомств никогда не звонят по мессенджерам, в том числе по WhatsApp, Telegram. ЛЮБОЙ ЗВОНОК ЧЕРЕЗ мессенджеры (WhatsApp, Telegram и т.д.) – ЭТО ПРИЗНАК МОШЕННИЧЕСТВА.

Не надо сообщать по телефону сведения (коды) из смс-сообщений, не надо переходить по их просьбе по различным ссылкам и не надо скачивать в мобильный телефон сомнительные приложения и программы. Надо прервать разговор, для проверки информации необходимо обратиться в ближайший отдел полиции или на горячую линию МВД по номеру «102».

Еще совет при возможности установить через портал Госуслуг самозапрет на оформление кредитов.

Какова статистика раскрываемости преступлений, связанных с дистанционным мошенничеством? Расскажите об успешных практиках раскрытия такого рода уголовных дел.

Раскрываемость преступлений дистанционных мошенничеств остается невысокой.

Низкая раскрываемость напрямую связана с тем, что мошенники преимущественно работают из других стран, а их телефоны и компьютеры недоступны

нашим правовым структурам, из-за этого установить личность преступника и его местонахождение сложно. Кроме того, мошенники часто используют анонимизирующие технологии и шифрование, что значительно осложняет процесс отслеживания их действий и сбора доказательств.

Тем не менее, работа по раскрытию преступлений рассматриваемой категории у нас проводится.

Например, сотрудниками управления по борьбе с кибермошенничествами МВД по Республике Саха (Якутия) в ходе оперативных мероприятий по раскрытию мошенничества, совершенного в отношении жителя Якутии, установлены 2 лица, которые принимали участие в преступной схеме «инвестиции» в качестве «дроповодов» и поступившие денежные средства переводили в криптокошельки участников организованной преступной группы.

В ходе изучения изъятых сим-карт и банковских карт в подсистеме ИБД-Ф «Дистанционное мошенничество» установлены данные об использовании данных средств при совершении и иных преступлений на территории РФ (всего 75 эпизодов). Общая сумма похищенных средств составила более 60 млн. руб.

Уголовное дело по обвинению данных лиц в 2025 году направлено в суд для рассмотрения по существу.

Что делать человеку, если он уже стал жертвой мошенника? Какие меры предпринять?

Если гражданин стал жертвой телефонного мошенничества, ему в первую очередь необходимо обратиться в полицию с соответствующим заявлением. В заявлении следует максимально подробно рассказать о всех обстоятельствах.

Необходимо незамедлительно заблокировать карту, чтобы мошенники потеряли доступ к оставшимся на ней деньгам. Сделать это можно разными способами: через мобильное приложение банка, по телефону горячей линии, по СМС, в отделении банка.

При необходимости можно обратиться в банк и попытаться оспорить операцию. В некоторых случаях, клиенту должны вернуть деньги за перевод, совершенный без его согласия. Если человек не нарушал правила безопасности при использовании платежных средств, банк должен провести расследование и вернуть деньги. Этот способ не подойдет, если деньги были отправлены мошенникам добровольно.