

Информация
о состоянии оперативной обстановки на территории
Магаданской области, связанной с преступлениями, совершёнными
с использованием информационно-телекоммуникационных технологий, и
новых способах совершения киберпреступлений

По итогам 2024 года оперативная обстановка в Магаданской области, связанная с преступлениями, совершёнными с использованием информационно-телекоммуникационных технологий (далее – ИТТ), характеризуется следующими показателями.

Рост числа преступлений рассматриваемой категории был отмечен во всех муниципальных образованиях, за исключением Ольского и Северо-Эвенского муниципальных округов:

Таблица № 1. Число зарегистрированных преступлений с использованием ИТТ в 2023 – 2024 годах.

Муниципальное образование	2023 г.	2024 г.	Динамика, +,-%
Город Магадан	742	772	+4,0
Сусуманский муниципальный округ	18	19	+5,6
Ягоднинский муниципальный округ	23	29	+26,1
Хасынский муниципальный округ	28	31	+10,7
Среднеканский муниципальный округ	5	6	+20,0
Омсукчанский муниципальный округ	13	21	+61,5
Тенькинский муниципальный округ	7	17	+142,9
Ольский муниципальный округ	35	21	-40,0
Северо-Эвенский муниципальный округ	6	3	-50,0
Всего	877	919	+4,8

Наиболее негативная динамика отмечена в Тенькинском (+142,9%) и Омсукчанском (+61,5%) муниципальных округах. На рост общего массива ИТ-преступлений (+4,8%) безусловно повлияла ситуация в областном центре (+4,0%), где в 2024 году совершено 84% всех противоправных деяний.

Значительную часть от числа ИТ-преступлений в 2024 году составили мошенничества и кражи (60,3%). По итогам прошедшего года число

мошенничеств снизилось на 10,6%, краж – на 2,9%.

Таблица № 2. Число зарегистрированных мошенничеств и краж с использованием ИТТ в 2023 – 2024 годах.

Муниципальное образование	Мошенничества			Кражи		
	2023 г.	2024 г.	+/- %	2023 г.	2024 г.	+/- %
Город Магадан	369	318	-13,8	132	130	-1,5
Сусуманский муниципальный округ	9	11	+22,2	4	5	+25,0
Ягоднинский муниципальный округ	16	15	-6,3	4	7	+75,0
Хасынский муниципальный округ	14	16	+14,3	12	7	-41,3
Ольский муниципальный округ	13	11	-15,4	16	5	-68,8
Среднеканский муниципальный округ	4	1	-75,0	1	3	+200,0
Омсукчанский муниципальный округ	9	12	+33,3	0	2	+100,0
Северо-Эвенский муниципальный округ	3	2	-33,3	1	0	-100,0
Тенькинский муниципальный округ	2	8	+300,0	1	7	+600,0
Всего	434	388	-10,6	171	166	-2,9

Вместе с тем число кибермошенничеств увеличилось в Сусуманском (+22,2%), Хасынском (+14,3%), Омсукчанском (+33,3%) и наиболее существенно – в Тенькинском (+300%) муниципальных округах. Соответственно количество краж с использованием ИТТ возросло в Сусуманском (+25,0%), Ягоднинском (+75,0%), Среднеканском (+200,0%), Омсукчанском (+100,0%) и в Тенькинском (+600%) муниципальных округах.

В два раза возросла раскрываемость мошенничеств: с 5,2% в 2023 году до 14,8% по итогам 2024 года. Удельный вес раскрытых краж существенно выше – 43,2% (2023 г. – 44,6%).

Материальный ущерб от преступлений рассматриваемой категории по сравнению с 2023 годом несколько снизился и составил 248 млн 732 тыс. рублей (2023 г. – 268 млн 852 тыс. рублей).

Несмотря на отдельные позитивные изменения в структуре преступности, связанной с кибермошенничествами и кражами, отмеченными в 2024 году, в текущем году наметился ряд негативных тенденций.

Так, общий массив преступлений, совершённых с использованием ИТТ, вырос по области более чем на треть (+36,3%):

Таблица № 3. Число зарегистрированных преступлений с использованием ИТТ за 2 месяца 2024 и 2025 годов.

Муниципальное образование	2 мес. 2024 г.	2 мес. 2025 г.	+/- %
Город Магадан	84	111	+32,1
Сусуманский муниципальный округ	0	3	+100,0
Ягоднинский муниципальный округ	3	5	+66,7
Хасынский муниципальный округ	0	8	+100,0
Ольский муниципальный округ	7	8	+14,3
Среднеканский муниципальный округ	3	0	-100,0
Омсукчанский муниципальный округ	5	1	-80,0
Северо-Эвенский муниципальный округ	0	1	+100,0
Тенькинский муниципальный округ	0	2	+100,0
Всего	102	139	+36,3

Как видно из таблицы, рост их числа отмечен во всех муниципальных образованиях, кроме Омсукчанского муниципального округа.

Также в текущем году отмечен рост кибермошенничеств и краж:

Таблица № 4. Число зарегистрированных мошенничеств и краж с использованием ИТТ за 2 месяца 2024 и 2025 годов.

Муниципальное образование	Мошенничества			Кражи		
	2 мес. 2024 г.	2 мес. 2025 г.	+/- %	2 мес. 2024 г.	2 мес. 2025 г.	+/- %
Город Магадан	41	41	0	13	28	+115,4
Сусуманский муниципальный округ	0	2	+100,0	0	0	+100,0
Ягоднинский муниципальный округ	1	5	+400,0	1	0	-100,0
Хасынский муниципальный округ	0	4	+100,0	0	1	+100,0
Ольский муниципальный округ	2	3	+50,0	2	4	+100,0

Среднеканский муниципальный округ	0	0	-	2	0	-100,0
Омсукчанский муниципальный округ	4	0	-100,0	0	1	+100
Северо-Эвенский муниципальный округ	0	0	-	0	1	+100,0
Тенькинский муниципальный округ	0	1	+100,0	0	1	+100,0
Всего	48	56	+16,7	18	36	+100,0

Рассматривая личность потерпевших, УМВД России по Магаданской области отмечено, что счета мошенников в основном пополняют молодые трудоспособные граждане, люди грамотные, образованные, активные. Чаще других это – медики, педагоги, работники дошкольных учреждений, предприятий различных форм собственности, индивидуальные предприниматели и пенсионеры.

В настоящее время на территории Магаданской области наиболее распространены следующие способы совершения дистанционных преступлений:

1. Звонки от злоумышленников, которые обманным путём вводят в заблуждение потерпевших, представляясь сотрудниками банков, правоохранительных органов, операторов сотовой связи и т.д., в результате чего получают доступ к их счетам и списанию денежных средств.

2. Взлом учётной записи в мессенджерах, когда контактам потерпевшего якобы от его имени направляются сообщения с конечной просьбой занять в долг денежные средства.

3. «Покупка-продажа» имущества (предоставление услуг) через сайты объявлений (торговые интернет-площадки).

4. Возможность дополнительного заработка на фейковых биржах, якобы осуществляющих брокерскую и инвестиционную деятельность.

В настоящее время это один из самых распространённых схем мошенничества. Часто граждане пытаются «заработать» на бирже

«Газинвест», «Газпрома», при этом нередко жертвами мошенников становятся пенсионеры.

5. Взлом личного кабинета пользователей портала «Госуслуги» (квалифицируется как «неправомерный доступ к компьютерной информации»).

6. Преступная схема «родственник в беде».

7. Фейковые розыгрыши призов.

Чтобы не стать жертвой злоумышленников, необходимо соблюдать следующие правила безопасного поведения:

1. Не следует отвечать на звонки или СМС-сообщения с неизвестных номеров. Не перезванивайте на неизвестные номера. **ЗАЩИТИТЕ СВОЙ СМАРТФОН:**

- не устанавливайте на свой смартфон никаких программ по указанию неизвестных;

- в качестве помощи в борьбе с мошенниками целесообразно установить на личные мобильные устройства бесплатные услуги сотовых операторов по блокировке спам-звонков и идентификации звонящих (МегаФон – «Помощник Ева», МТС – «Защитник», Билайн – «Виртуальный помощник», Т2 – «Антиспам для звонков» и другие).

2. Ни при каких обстоятельствах не сообщайте реквизиты своих банковских счетов и карт, пароли от них и тем более не перечисляйте принадлежащие вам денежные средства по указанию лиц, представляющихся сотрудниками банков (службы безопасности банков) и правоохранительных органов (полиция, ФСБ, Росфинмониторинг и т.д.), на безопасные счета! Понятия «БЕЗОПАСНЫЙ СЧЁТ» НЕ СУЩЕСТВУЕТ! Немедленно прервите разговор!

3. Не берите кредиты якобы для того, чтобы опередить злоумышленников. **ТАКОГО СПОСОБА ЗАЩИТЫ ВАШИХ СРЕДСТВ НЕ СУЩЕСТВУЕТ!**

4. В случае поступления сообщения от родственника, знакомого, руководителя (коллег по работе) с просьбой занять денег или с информацией о том, что вам скоро позвонят из органов безопасности или Центробанка РФ и следует действовать по их инструкции, САМОСТОЯТЕЛЬНО СВЯЖИТЕСЬ С ТЕМ, КТО ПРОСИТ ОКАЗАТЬ ПОМОЩЬ, И УТОЧНИТЕ СИТУАЦИЮ.

5. ОБРАТИТЕ ВНИМАНИЕ! НЕ СОЗВАНИВАЮТСЯ С КЛИЕНТАМИ:

- сотовые компании – с целью продления услуг мобильной связи (работа ведётся исключительно через официальное мобильное приложение операторов связи);

- Отделение Фонда пенсионного и социального страхования Российской Федерации по Магаданской области (его филиалы) – с предложением услуг по перерасчёту размера пенсии и трудового стажа;

- АО «Магаданэнергосбыт» – для оказания содействия по замене счётчика электроэнергии либо настройки личного кабинета на сайте компании;

- медицинские организации – об оказании услуги по дистанционной записи в очередь на замену полиса обязательного медицинского страхования.

6. При совершении ОНЛАЙН-ПОКУПОК ИЛИ ПРОДАЖ НА ИНТЕРНЕТ-ПЛОЩАДКАХ объявлений следуйте следующим рекомендациям:

- изучите карточку продавца, его рейтинг и отзывы. Насторожитесь, если продавец имеет слишком низкий рейтинг и большое количество отрицательных отзывов;

- мошенники часто используют фишинговые сайты, замаскированные под реально существующие онлайн-ресурсы торговых площадок (доменное имя при этом может отличаться всего лишь одним символом). Ссылки на фишинговые сайты, как правило, оставляют в мессенджерах, поэтому

общайтесь с пользователями только через чат интернет-площадки размещения объявлений. В большинстве случаев в таких чатах блокируется рассылка ссылок. Если ресурс не блокирует ссылки, отправляемые пользователям, просто не переходите по ним;

- мошенники часто пытаются увести вас с интернет-ресурса. Следует настороженно отнестись к просьбам продолжить общение в WhatsApp, Viber, Telegram. Вас могут убеждать в том, что функционал сайта работает некорректно, и сделку лучше совершить в обход ресурса. Никогда не поддавайтесь на подобные уговоры. Оплату проводите только через платёжные сервисы, которые предлагает выбранная вами интернет-площадка. В таком случае вы можете быть уверены в безопасности оплаты и в сохранности денежных средств на вашей карте. Поскольку сервисы безопасной оплаты предполагают блокирование денег на виртуальном счету торговой площадки, в случае неполучения товара или получения товара ненадлежащего качества денежные средства вернутся на ваш счёт. Только при подтверждении получения нужного вам заказа и отсутствии претензий к его качеству торговая площадка направляет денежные средства продавцу.

- не отправляйте предоплату за товар или услугу;

- при общении в чате мошенники под самыми разными предлогами могут попытаться получить информацию, позволяющую совершать несанкционированные операции с вашей банковской картой. Поэтому ни при каких обстоятельствах не сообщайте пользователям код на обратной стороне карты (CVV/CVC-код), а также коды из СМС-сообщений для совершения оплаты, приходящих на номер вашего сотового телефона.

- если вы всё же успели ввести номер своей карты на поддельном сайте или передать свои платёжные данные мошенникам и только потом поняли — что-то не так, нужно немедленно позвонить в банк, заблокировать карту и подать заявление на её перевыпуск. Если успеете сделать это до того, как мошенники воспользуются вашими данными, потери денег удастся избежать.

7. Не следует доверять звонкам и сообщениям, о том, что РОДСТВЕННИК ИЛИ ЗНАКОМЫЙ ПОПАЛ В АВАРИЮ, ЗАДЕРЖАН ЗА СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЯ, особенно, если за этим следует просьба о перечислении денежных средств. Как показывает практика, обычный звонок близкому человеку позволяет развеять сомнения и понять, что это мошенники пытаются завладеть вашими средствами или имуществом.

8. Чтобы не допустить несанкционированный доступ в ваш личный кабинет на сайте «Госуслуги», необходимо соблюдать ряд простых правил кибербезопасности, которые изложены на официальном этого сайта (ссылка: https://www.gosuslugi.ru/help/faq/personal_data/100465). Особое внимание специалисты по кибербезопасности обращают внимание на создание уникального пароля для входа в личный кабинет из 12 символов (ссылка: https://www.gosuslugi.ru/life/details/how_to_create_strong_passwords).

9. Общая рекомендация: предупредите родственников и знакомых, особенно лиц пожилого возраста, о существующих способах мошенничества.

Следует обратить внимание, что в Магаданской области появились новые способы мошенничества, которые довольно распространены в центральных районах страны.

1. Так, МВД России отмечает, что последнее время участились случаи, когда интернет-мошенники запугивают граждан статьёй из Уголовного кодекса Российской Федерации о госизмене из-за финансирования Вооружённых сил Украины.

Суть обмана следующая. Вам звонит якобы сотрудник ФСБ или полиции, который сообщает, что некий нечестный банковский служащий украл ваши персональные данные и произвёл от вашего имени переводы в пользу Вооружённых сил Украины. Формально переводы якобы совершаются от вашего имени, что грозит возбуждением уголовного дела за государственную измену и (или) содействие террористической деятельности.

Некоторые доверчивые граждане, услышав подобное, сразу пугаются. И тут звонивший предлагает схему, которая позволит снять с вас обвинения в

госизмене. Для этого нужно помочь службе безопасности банка найти злоумышленника. Нужно сделать один или лучше несколько переводов на некие надежные счета, и якобы эти действия помогут поймать преступника. В реальности доверчивые граждане переводят деньги настоящим мошенникам.

По другой преступной схеме вы неожиданно получаете на свою банковскую карту денежный перевод, а в комментариях мошенники пишут благодарность за помощь якобы Вооружённым силам Украины. Затем преступники делают скриншот сообщения о переводе денежных средств и обещают отправить снимок в органы безопасности. И хотя гражданина России не могут привлечь в данном случае к какой-либо ответственности, ситуация рассчитана на особо восприимчивых лиц, которые в стрессовой ситуации обязательно обратятся в правоохранительные органы. Таким образом вырастает нагрузка на полицию и органы безопасности, и на фоне большого потока бесполезной информации по-настоящему важные сообщения о преступлениях или тех же донатах в пользу ВСУ потеряются.

Так, в марте 2025 года жертвой мошенников стал учитель одной из общеобразовательных учреждений Магаданской области. В заявлении о преступлении, поступившем в дежурную часть органов внутренних дел, указано, что потерпевшему поступило по мессенджеру «Вотсап» сообщение о том, что заявитель якобы осуществляет финансирование Вооруженных сил Украины, при этом, возможно, потерпевший об этом факте не знает, и перевод денежных средств происходит без его участия. Чтобы обезопасить себя от попыток хищения со стороны иных лиц, заявителю было предложено установить на смартфон защитную программу, которая в тоге после установки, напротив, позволила злоумышленникам обеспечить доступ к банковским счетам жертвы. После установки приложения, воспользовавшись удаленным доступом, злоумышленник убедил перевести денежные средства в сумме 250 000 рублей в другой банк, а затем деньги были обналичены преступниками.

Рекомендация в данном случае одна: если гражданин вдруг получает подобный звонок, необходимо сразу прервать разговор и сообщить о случившемся в полицию.

2. Всё чаще в регионе стали регистрироваться мошеннические схемы, связанные с деятельностью «Почты России», когда представитель якобы этой организации звонит Вам и под тем или иным предлогом выманивает информацию, которая способствует завладению вашими денежными средствами либо получению доступа к вашему личному кабинету сайта «Госуслуги».

Схема мошенничества выглядит следующим образом: жертве звонят от имени якобы сотрудника «Почты России» и предлагают получить заказное письмо лично или в электронном виде. Часто, например, речь может идти о получении *писем из налоговой инспекции*. Если человек выбирает электронный вариант, мошенники могут назвать его настоящий адрес электронной почты, чтобы вызвать доверие. Затем злоумышленники предлагают воспользоваться якобы существующим «чат-ботом» для получения письма.

Вот лишь несколько таких примеров по Магаданской области.

1) В марте 2025 года в дежурную часть ОМВД России по г. Магадану поступило заявление от работника одного из салонов, осуществляющих бьюти-услуги в областном центре, о том, что неустановленное лицо, путем обмана под предлогом подтверждения почтового отправления, представившись сотрудником «Почта России», убедило заявителя продиктовать код из «СМС-сообщения», направленный на абонентский номер заявителя, в результате чего был заблокирован доступ к личному кабинету потерпевшего на портале «Госуслуги».

2) В марте 2025 года дежурную часть ОМВД России по г. Магадану поступило заявление от жителя областного центра, работника одного из областных государственных бюджетных организаций о том, что неустановленное лицо, используя звонок в мессенджере ««WhatsApp» путём

обмана, представившись сотрудником «Почты России», под предлогом получения письма из министерства дорожного хозяйства Магаданской области, убедило заявителя перейти по ссылке в мессенджер Telegram на страницу бота «Почта России» («@RusPost_RoBot») и ввести логин и пароль от сайта «Госуслуги», после чего совершило неправомерный доступ к компьютерной информации, а именно завладело аккаунтом заявителя на портале «Госуслуги», осуществило его модификацию, блокировку, ограничив доступ к его восстановлению. В дальнейшем заявителю позвонила женщина, которая представилась сотрудником банка, и введя в заблуждение, убедила через систему быстрых платежей перечислить денежные средства в сумме 133 000 рублей (кредитные) на предоставленный абонентский номер. «А»).

Важно знать: Почта России никогда не звонит клиентам, тем более по мессенджеру «Вотсап» (преступники используют подменные номера, идентифицирующиеся в смартфоне при соединении как «Почта России») и не запрашивает коды из СМС-сообщений. Если гражданин вдруг получает подобный звонок, его срочно надо прервать.

Об этих и других способах мошенничества и как противостоять им, можно узнать из «Вестника Киберполиции России», созданного Управлением по организации борьбы с противоправным использованием информационно-телекоммуникационных технологий МВД России на страницах социальной сети «ВКонтакте» (ссылка: https://m.vk.com/cyberpolice_rus) и в Telegram-канале (ссылка: https://t.me/cyberpolice_rus).

Рекомендуется подписаться на эти ресурсы для получения актуальной информации, ссылки разместить на сайтах администраций муниципальных образований Магаданской области в разделах по профилактике киберпреступлений.
