Криминологические характеристики в сфере противодействия дистанционных хищений денежных средств за 6 месяцев 2023 года на территории Челябинской области:

За июнь 2023 года число зарегистрированных на территории Челябинской области краж и мошенничеств в сфере информационно-телекоммуникационных технологий возросло на 25,67% (с 4768 до 5992; + 1224 преступления).

Данная ситуация обусловлена динамикой роста регистрации мошенничеств +24,87% (с 3650 до 4558; +908 преступлений).

1. Преступления совершены:	Доля потерпевших от общего количества потерпевших от ДМ
Под видом сотрудника банка, сотрудника правоохранительных органов	45,3 %
Объявления с рекламой об оказании услуг, о покупке-продаже на Интернет порталах бесплатных объявлений, в Интернет-магазинах, в социальных сетях, а также на ресурсах по пассажироперевозкам	16%
Оформление кредита в микрофинансовых организациях, банке посредством использования недостоверных данных или без намерений его выплаты.	16,6%
Помощь родственнику, который якобы попал в дорожно - транспортное происшествие.	9,2 %
Под предлогом инвестирования на бирже, вложения в криптовалюту.	9,8 %
Взлом аккаунта в социальных сетях.	1,4%
Под предлогом возврата или компенсации денежных средств за ранее приобретённые биологически активнне добавки (БАДы)	0,5 %
Иные способы (под предлогом оказания интимных услуг, обучение на курсах).	0,5 %
Оформление кредита в микрофинансовых организациях, банке без ведома потерпевшего.	0,4 %
Хищение денежных средств с использованием реквизитов банковской карты, которые ранее использовались владельцем карты при продаже/покупке через Интернет.	0,3 %
2. Возрастные категории потерпевших:	
До 20 лет.	1,2%
От 21 года и до 35 лет.	19%
От 36 лет и до 50 лет.	38,4 %
От 51 года и до 70 лет.	32,8 %
От 71 года и старше.	8,6 %
3. Род занятий потерпевшего:	
Учащийся, студент.	1,1 %

Государственные служащие, сотрудники бюджетной сферы.	4,9 %
Работники коммерческих организаций.	45%
Юридические лица, индивидуальные предприниматели, самозанятые.	15,8%
Пенсионеры.	18,8%
Безработные.	14,4 %
Пол	
Женский	41,5%
Мужской	58,5 %

На территории Челябинской области увеличилось количество дистанционных хищений денежных средств, совершенных с использованием неправомерного доступа к учётным записям на портале Государственных услуг: так, с начала 2023 года зарегистрировано 768 преступлений данной категории (ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»). Способ совершения указанных противоправных действий показывает, что фактически злоумышленники посредством методов «социальной инженерии» при общении (в том чисел, с использованием мессенджеров WhatsApp или Viber с установленным фото профиля в виде официального логотипа Портала) с владельцем учётной записи получают от него коды доступа к учётной записи, отправляемые для восстановления доступа. После получения кодов злоумышленник изменяет как пароль доступа к учётной записи, так и контрольный вопрос для восстановления пароля, из-за чего фактический владелец учётной записи лишается доступа к ней. Далее злоумышленник с использованием персональных данных фактического владельца учётной записи совершает в отношении него заведомо противоправные действия - оформление кредита в финансово-кредитных организациях, регистрация сим-карт.

Наиболее распространённые способы совершения мошенничеств с использованием информационно-телекоммуникационных технологий:

1. Под предлогом оказания содействия родственнику, якобы попавшему в дорожно-транспортное происшествие или якобы задержанному правоохранительными органами. Денежные средства потерпевший передаёт прибывшему к нему курьеру, который в дальнейшем перечисляет полученные денежные средства на указанные мошенниками банковские счета, при этом 15% оставляя себе.

2. Представляясь сотрудником банка, полиции, прокуратуры, ФСБ, Следственного комитета. Мошенник используя IP телефонию звонит потерпевшему с подменных номеров (номерная емкость начинается с 8800, 495, 499, а также с использованием номеров телефонов реально существующих ведомств, организаций, государственных органов, применяя специальное оборудование) и информирует гражданина о подозрительных финансовых операциях по его банковскому счету, попытках оформления кредита, перевода денежных средств со счёта, либо сообщает о розыске, задержании преступников, совершающих хищения денежных средств с расчетных счетов граждан, при этом извещает о необходимости соблюдения «тайны следствия». Далее, используя методы психологического воздействия и пользуясь доверчивостью граждан, вынуждает

потерпевшего сообщать персональные данные, сведения о финансовом состояния, о наличии автотранспорта в собственности. Затем под манипулятивным воздействием мошенника, потерпевший переводит денежные средства на якобы безопасные расчетные счета (в отдельных случаях, переводят деньги, вырученные от срочной продажи автотранспорта, недивижимости. Сделку по срочной продаже имущества организуют сами мошенники). Потерпевшие: все категории граждан, независимо от пола, образования, экономического, национального, социального статуса, а также возраста.

3. Под предлогом дополнительного заработка, участия в торгах на бирже, инвестирования в ценные бумаги. Граждан заманивают яркими вывесками, названиями созвучными с названиями крупных нефте/газодобывающих компаний и холдингов, таких как Газпроминвестии, ТинькоффИнвест, «исключительными» предложениями, возможностью получения высокого дохода, вынуждают потерпевшего вносить крупные суммы, без возможности вывода денежных средств в дальнейшем. Потерпевшие: все категории граждан, независимо от пола, образования, экономического, национального, социального статуса, а также возраста.

4. С использованием торговых площадок Авито, Юла, объявлений о купле/продаже в социальных сетях:
- путем размещения «фиктивного» объявления о продаже товара по цене значительно ниже рыночной. Как правило, переписка между покупателем и мошенником ведется на торговой площадке либо с использованием мессенджеров WhatsApp, Telegram, Viber. В ходе общения мошенник «входит» в доверие и вынуждает жертву оплатить товар полностью либо внести предоплату путем электронных переводов. После оплаты контакты с покупателем прекращаются, его блокируют, объявление удаляют.
- хищения денежных средств под предлогом покупки товара. В данном случае переписка между продавцом и мошенником также ведется с использованием сообщений на сайте, либо с использованием мессенджеров WhatsApp, Telegram,Viber. Продавца убеждают направить товар Авито, Юла доставкой, сообщая, что товар оплачен, и для получения денежных средств необходимо перейти по ссылке, которую скидывают на телефон продавца. После перехода по ссылке продавец попадает на фишинговый сайт Авито, Юла, где вносит свои персональные данные и реквизиты банковской карты, сумму для получения. После нажатия на «окно» «Получить деньги», денежные средства списываются с расчетного счета продавца. Кроме того, в дальнейшем мошенники убеждают продавца, что произошел сбой и для возврата денежных средств необходимо обратиться в службу поддержки, перейдя по ссылке. Продавец, перейдя по ссылке, вновь попадает на фишинговый сайт, где указывает свои данные, реквизиты карты и сумму, якобы необоснованно списанную. После нажатия на «окно» получить деньги, с расчетного счета продавца повторно списываются денежные средства. Таким же способом совершается хищение денежных средств через сайт по поиску попутчиков («BlaBlaCar»): мошенники размещают объявления с предложением услуги по пассажироперевозке. Когда пользователь откликается на объявление, мошенник в чате на сайте BlaBlaCar просят его связаться с ним в WhatsApp по определённому номеру телефона. Затем, в ходе переписки в WhatsApp клиенту предлагают оплатить поездку и скидывают ему ссылку на фишинговый сайт для оплаты поездки. После перехода на сайт, пользователь вводит реквизиты своей банковской карты, далее денежные средства списываются на счёт мошенники.

5. Хищение денежных средств с использованием социальных сетей. От имени

потерпевшего его знакомым, друзьям, родственникам приходит сообщение с просьбой одолжить денежные средства. Также злоумышленники рассылают сообщение о сборе денежных средств на лечение больного ребенка, похороны и т. д.

6. Оформление кредита в микрофинансовых организациях без ведома потерпевшего. Хищение осуществляется путём перебора сим-карт для поиска активного акканута заёмщка и использование личного кабинета лица, ранее оформлявшего в микрофинансовых организациях заём.

7. Под предлогом получения возврата или получения компенсации денежных средств за ранее приобретенные биологически активные добавки (БАДы): мошенники, представляясь сотрудниками правоохранительных органов, в телефонном разговоре с потерпевшим сообщают тому, что органов, в телефонном разговоре с потерпевшим сообщают тому, что задержали преступников, занимавшихся ранее продажей некачественных пищевых добавок. Для получения компенсации необходимо оплатить налог, открытие счета, транзакцию и т.п. В результате граждане, рассчитывая получить компенсацию, перечисляют мошенникам денежные средства, сумма которых превышает сумму обещанной компенсации.

Ущерб от преступлений данного вида по итогам первого полугодия 2023 года составил 1 000 062 295 рублей.

Указанные сведения о результатах анализа совершённых дистанционных мошенничеств, а также информация о наиболее распространённых схемах совершения преступлений, могут быть использованы при организации информационно-разъяснительной работы в трудовых коллективах, разработке адресного информационного контента.