«Предупреждение мошенничеств и иных противоправных деяний, совершаемых посредством глобальной компьютерной сети «Интернет», а также телефонной связи»

Актуальность рассматриваемой проблемы обусловлена тем, что информационная среда (интернет) в общем и информационно-коммуникационные технологии (далее - ИКТ) в частности, благодаря глубокому проникновению практически во все сферы жизнедеятельности граждан, общества и в целом государства в наши дни стали площадкой для совершения различного рода преступлений. Процесс возникновения новых способов совершения преступлений, модификации и совершенствования старых способов идет параллельно развитию технологий и уровню их интеграции в реальную жизнь.

В настоящее время ИКТ преимущественно применяются для совершения преступлений против собственности в целом, а в частности - мошенничеств.

Рост числа совершенных мошенничеств наблюдается на протяжении ряда последних лет во всех регионах республики.

Основной причиной, обусловившей сложившуюся криминогенную обстановку, непосредственно является активное использование при подготовке и совершении преступлений ИКТ, позволяющих сохранить анонимность, в кратчайшие сроки распорядиться похищенным имуществом, скрыть следы преступления и в целом обеспечить безопасность благодаря удаленности от места наступления преступных последствий. На основании имеющихся данных, в ближайшем будущем прогнозируется устойчивый рост преступлений данного вида.

Самым распространенным и наименее затратным для преступника способом совершения мошенничества в сети Интернет является размещение на различных онлайн-ресурсах объявлений о реализации различного рода товаров (услуг) и завладение денежными средствами, поступающими в счет их оплаты, без намерения реального осуществления договорных обязательств.

Преступниками активно используются методы социальной инженерии (совокупность психологических приемов, служащих для получения конфиденциальных данных, либо побуждающих к совершению определенных действий).

Характерным примером преступлений, совершенных данным способом, являются звонки «сотрудников служб безопасности банков» и «представителей правоохранительных органов». В данном случае потерпевших убеждают в том, что с использованием их персональных данных преступники с помощью недобросовестных работников банковский учреждений пытаются заключить кредитные договоры. С целью обеспечения сохранности денежных средств и изобличения преступников им самим необходимо срочно получить кредит на

определенную сумму, чтобы последующие заявки не были одобрены. Кредитные средства необходимо перечислить на «защищенный счет», чтобы в последствии не исполнять обязательства по кредитному договору.

С 2022 года на территории республики получил распространение вид мошенничества, связанный с завладением денежными средствами под предлогом оказания помощи близким родственникам, попавшим в экстремальную ситуацию. Злоумышленник, осуществляя звонок на стационарный телефон, представляясь близким родственником потерпевших, сообщал, что стал виновником дорожно-транспортного происшествия и для возмещения ущерба и непривлечения к ответственности необходимо выплатить определенную сумму денег. При общении по телефону злоумышленник создает впечатление реальности сообщаемых сведений (плач, крики, голоса третьих лиц), в результате чего потерпевшие, находясь в стрессовом состоянии, соглашаются с требованиями неизвестных передать денежные средства курьеру. Имели место случаи, когда факт совершения ДТП подтверждал сообщник мошенника, представляясь потерпевшему сотрудником правоохранительных органов. Злоумышленник для правдоподобности передаваемой информации предлагает потерпевшим написать заявление о непривлечении близкого родственника к уголовной ответственности, а также, в ходе разговора, длительное время удерживает потерпевшего на связи с целью предоставления сообщнику (курьеру) времени покинуть место преступления.

Также необходимо иметь ввиду, что «Интернет» - публичное место, и все, что когда-либо размещено в сети, потенциально может быть доступно неограниченному числу пользователей. Распространение конфиденциальной информации, которую потерпевшие хотели бы сохранить в тайне, становится предметом торга вымогателей.

Раскрытие преступлений, совершаемых с использованием ИКТ, затрудняется тем, что преступники пользуются интернет-ресурсами, не входящими в национальный сегмент сети. Получение необходимых сведений зачастую по объективным причинам невозможно либо на это уходит очень много времени, которое используется преступниками для уничтожения следов своей активности.

В силу указанных причин одним из действенных способов борьбы с преступлениями данного вида является разъяснительная работа с населением и повышение общего уровня цифровой грамотности.

Вместе с тем, обезопасить себя от преступных действий в сети достаточно просто. Для этого необходимо соблюдать ряд простейших правил:

- серьезно относиться к сохранности персональных данных (номера телефонов, банковских карт, личных документов и т.д.);

- никому, никогда ни при каких условиях не сообщать платежные реквизиты банковских карт, данные, необходимые для авторизации в системах дистанционного банковского обслуживания, коды подтверждения операций и т.д.;

- соблюдать цифровую гигиену: не посещать сомнительные сайты, не использовать одинаковые логины и пароли для регистрации на разных интернет-площадках, использовать разные почтовые ящики для переписки с официальными структурами, дружеской переписки, интернет коммерции и т.д., там, где это возможно, использовать двухфакторную аутентификацию;

- не использовать для покупок в сети «зарплатную» банковскую карту, а на используемой установить лимиты по количеству и сумме операций и подключить дополнительные средства обеспечения безопасности (3D- secure и т.д.);

- помнить о том, что «на другом конце провода» может находиться кто угодно и не доверять незнакомым собеседникам вне зависимости от того, кем они представляются, при получении странной либо необычной просьбы в сообщении даже от близких родственников и друзей перепроверить информацию альтернативным способом;

- отдавать себе отчет в том, что, приобретая товар по объявлению в социальной сети, вы действуете на собственный страх и риск, отдавать предпочтение приобретению товаров на специализированных торговых площадках, обеспечивающих безопасность платежа, доставку товара и гарантию возврата денежных средств при получении товара ненадлежащего качества или его не получения.

Отделение уголовного розыска
криминальной милиции Мядельского РОВД