**Об уголовной ответственности за хищения, совершенные с использованием информационно-коммуникационных технологий**

Динамика развития информационных технологий в последние годы влечет повсеместное их вовлечение во многие сферы общественных отношений, что влечет не только удобство для добросовестных пользователей, но и почву для противоправной деятельности, выражающейся в незаконном обогащении, дискредитации граждан и государственных органов, распространении запрещенной информации, в том числе, идей экстремизма и терроризма.

Как в целом по стране, так и на территории Челябинской области, отмечается ежегодный рост таких преступлений, к которым также относятся хищения денежных средств из банков и иных кредитных организаций (физических и юридических лиц), совершаемых с использованием современных информационно-коммуникационных технологий.

Ответственность за совершение таких деяний, в зависимости от способа совершения преступлений, предусмотрена ст.ст. 158, 159, 159.3, 159.6 УК РФ.

С целью усиления уголовной ответственности, Федеральным законом от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» Уголовный кодекс РФ дополнен п. «г» ч. 3 ст. 158 УК РФ, которым за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ) предусмотрено наказание до 6 лет лишения свободы.

По тем же основаниям изменены диспозиции и санкции ст.ст. 159.3, 159.6 УК РФ, предусматривающие ответственность за противоправные действия с использованием электронных средств платежа.

Зачастую в совокупности с ними совершаются преступления в сфере компьютерной информации или так называемые киберпреступления, которые используются злоумышленниками в качестве инструмента завладения чужим имуществом: неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ), а также неправомерное воздействие на критическую информационную инфраструктуру РФ (ст. 274.1 УК РФ).

Подавляющее большинство анализируемых хищений совершается с применением методов «социальной инженерии», то есть доступа к информации с помощью телекоммуникационных сетей (сотовой связи, ресурсов сети Интернет). Данная преступная технология основана на использовании слабостей человеческого фактора и является достаточно эффективной.

Например, преступник может позвонить человеку, являющемуся пользователем банковской карты (под видом сотрудника службы поддержки или службы безопасности банка), и выяснить конфиденциальные данные банковской карты, сославшись на необходимость решения небольшой проблемы при работе в компьютерной системе или с банковским счетом, дезинформируя о его блокировке либо попытке совершения противоправных действий со стороны третьих лиц.

Также преступники зачастую представляются близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации. К примеру, в связи с необходимостью освобождения их от уголовной ответственности, разрешению в пользу близкого человека якобы виновного в ДТП, при этом нередко такие лица сами выдают себя за сотрудников правоохранительных органов.

Не менее распространены так называемые дистанционные формы хищения, совершаемые путем размещения на сайтах по продажам в сети Интернет заведомо ложных предложений о продаже товаров за денежное вознаграждение, которое в дальнейшем перечисляется на банковский счет виновного лица без фактической передачи приобретаемого товара либо предоставлении несоизмеримых по стоимости предметов.

Кроме того, нередко денежные средства неправомерно списываются со счетов потерпевших, когда в руки преступников попадают их мобильные телефоны с установленными на них банковскими сервисами или банковские карты: похитителями совершаются покупки путем оплаты товаров бесконтактным способом, при наличии пароля доступа - деньги снимаются в банкоматах.

В последние годы значительное распространение получил так называемый «фишинг» - один из методов «социальной инженерии», направленный на получение конфиденциальной информации, при котором злоумышленник посылает потерпевшему e-mail, подделанный под официальное письмо - от банка или платежной системы - требующее «проверки» определенной информации, или совершения определенных действий. Это письмо как правило содержит ссылку на фальшивую веб-страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести необходимую для преступников информацию - от домашнего адреса до пин-кода банковской карты.

Заместитель прокурора района

младший советник юстиции А.И. Бутрик