Противодействие преступлениям, совершенным с использованием информационно-коммуникационных технологий, является одним из приоритетных направлений деятельности правоохранительных органов области. Они посягают на права личности, создают угрозу национальной безопасности, причиняют имущественный ущерб гражданам, коммерческим структурам и бюджетной системе государства. Как правило данные преступления совершаются с территории других регионов России как в отношении граждан, предпенсионного и пенсионного возраста от 45 до 65 лет, так и более молодого возраста, в том числе детей.

Среди факторов, характеризующих активность преступников на данном направлении, можно выделить отсутствие непосредственного контакта с жертвой, свободное размещение информации самого различного свойства, в том числе криминального, доступ к ней неограниченного круга лиц и простоту ее сбора, анонимность пользователей, трансграничный характер информационно-телекоммуникационных сетей, возможность в этой связи охвата широкой аудитории и многие другое.

Не меньшее влияние в данной области оказывает активное развитие новых форм платных услуг и сервисов, а равно использование при расчетах цифровых средств платежей в отсутствие надлежащего государственного контроля и нормативного регулирования в «виртуальной» среде.

Такие преступления легче предотвратить, чем установить злоумышленников, которые с развитием информационных систем изобретают новые методы хищений денежных средств с использованием банковских карт, Интернет-магазинов, SMS-рассылок, лотерей, сайтов знакомств и брокерских контор.

Чтобы не стать жертвой посягательств в сфере информационно-коммуникационных технологий, следует знать схемы совершения таких преступлений.

Главный признак звонка от злоумышленника – вызов с незнакомого номера. Чаще всего мошенники притворяются сотрудниками ПАО «Сбербанка», ПАО «ВТБ», Центрального банка РФ, МВД РФ, Следственного комитета РФ, Генеральной прокуратуры РФ и пенсионным фондом.

При осуществлении вызова со стороны «сотрудников банка» злоумышленик будет рассказывать, что от имени клиента зарегистрирована заявка на смену доверенного номера или на оформление кредита. В случае МВД – собеседника могут обвинить в совершаемом им преступлении из-за переводов денежных средств в недружественные страны. «Специалисты» банка России будут убеждать собеседника срочно застраховать «единый лицевой счет» и иные счета, находящиеся в собственности клиента, а также осуществить перевод денежных средств на «безопасные счета». При звонкам пожилым гражданам злоумышленники представляются их родственниками и под предлогом совершения ими дорожно – транспортного происшествия, похищают денежные средства, за которыми как правило приезжают «курьеры», которые могут представляться помощниками следователей и сотрудников прокуратуры. Другие злоумышленники могут осуществлять звонки и предлагать вкладывать денежные средства путем инвестирования в

различные акции компаний и предприятий, таких как ПАО «Газпром», АО «Тинькофф банк», а также принять участие в покупке различной иностранной валюты, в том числе цифровой, на иностранных биржах и иных торговых площадках.

Кроме того, зафиксированы случаи, когда мошенники блокируют доступ в личный кабинет банковского учреждения, путем неверного ввода пароля к нему. В дальнейшем связываются с гражданином, представляются сотрудниками указанных кредитных организаций, сообщают сведения о том, что якобы зафиксированы случаи несанкционированного доступа к личному кабинету пользователя, который буду введенный в заблуждение предоставляет последним свои персональные данные, либо самостоятельно осуществляет переводы денежных средств на указанные последними якобы безопасные банковские счета.

Не менее распространенным преступным посягательством является неправомерный доступ к личным кабинетам граждан на портале «Госуслуги». В подобных случаях злоумышленники в телефонном режиме, представляясь сотрудниками мобильных операторов связи, банковскими работниками и др., введя жертву в заблуждение относительно причины звонка, просят сообщить код из SMS-сообщения, который используют для доступа к личному кабинет жертвы против ее воли и, как следствие, к персональным данным.

В связи с изложенным, ни при каких обстоятельствах нельзя переходить по сомнительным интернет-ссылкам, сообщать третьим лицам остаток денег на счетах, банковских картах, их номера, сроки действия, CVC/CVV-коды с оборота карт и из СМС-сообщений, приходящих с сервисных номеров банков и других организаций.

В случае поступления сомнительных звонков, подозрительных сообщений необходимо прекратить диалог и обратиться в полицию. Преступления в сфере информационно-коммуникационных технологий квалифицируются по ст.ст. 158, 159 УК РФ.