Преступления в сфере информационно-коммуникационных технологий в настоящее время приобретают особую актуальность.

В Российской Федерации предпринимаются дополнительные меры по обеспечению защиты информации в различных сферах правоотношений, порядок ее защиты регламентируется федеральными законами, в том числе:

- от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,

- от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»,

- от 27.07.2006 № 152-ФЗ «О персональных данных» (статья 19),

- от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (статья 27),

- от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния», а также постановлениями Правительства Российской Федерации, например, от 13.06.2012 № 584 «Об утверждении Положения о защите информации в платежной системе».

Предусмотрена и административная ответственность за правонарушения в области связи и информации. Так статья 13.12 КоАП РФ предусматривает ответственность за нарушение правил защиты информации, статья 13.13 КоАП РФ – за незаконную деятельность в области защиты информации, статья 13.14 КоАП РФ – за разглашение информации с ограниченным доступом. Кроме того, предусмотрена ответственность по статье 14.30 КоАП РФ за нарушение установленного порядка сбора, хранения, защиты и обработки сведений, составляющих кредитную историю, по статье 15.21 КоАП РФ – за неправомерное использование инсайдерской информации, по статье 17.13 КоАП РФ – за разглашение сведений о мерах безопасности.

Преступления данной категории чаще совершаются с применением расчетных пластиковых карт, с использованием компьютерной техники, сети «Интернет», а также средств мобильной связи. К ним относятся преступления против собственности, общественной безопасности, террористической и экстремистской направленности, против здоровья населения и общественной нравственности, в сфере компьютерной информации, против основ конституционного строя и безопасности государства, предусмотренные главами  21, 24, 25, 28, 29 Уголовного кодекса Российской Федерации.

Активное использование социальной сети может привести к наступлению негативных последствий для самих пользователей. В целях достижения желаемого результата злоумышленники с использованием информационно-телекоммуникационной сети «Интернет» могут осуществлять:
сбор общей информации о пользователе сети «Интернет» (фото, увлечения, трудовая деятельность, поездки, часто посещаемые места и маршруты). В связи с неиспользованием настроек конфиденциальности указанная информация становится легкодоступной для каждого лица,
использование лицами с какими-либо отклонениями сайтов знакомств, посредством которых могут быть совершены преступления в отношении несовершеннолетних, поиск в социальных сетях социально-незащищенных категорий граждан, тяжелобольных людей, которые в случае совершения в отношении них грабежа, мошенничества не смогут оказать активного сопротивления либо идентифицировать мошенника, определение с использованием геолокации пути жертвы в целях установления отсутствия лиц в доме, квартире. В данном случае преступник имеет возможность совершить проникновение в жилое помещение или хищение транспортного средства в отсутствии его собственника, использование социальных сетей в качестве инструмента для совершения призывов к чему-либо.

В целях недопущения вышеуказанных обстоятельств, необходимо быть бдительными, а также не поддаваться на уговоры незнакомых лиц, которые просят совершить определенные действия под диктовку, проверять самостоятельно поступающую от них информацию, найти официальные контактные данные банка, обратиться к специалистам для уточнения информации, сообщить в службу безопасности о поступающих звонках с указанием номеров абонентов,
не сообщать никому свои персональные данные, реквизиты банковских карт, логины и пароли от личных кабинетов, не осуществлять предоплату по частным объявлениям на сайтах, незнакомые номера добавить в «черный список» контактов.

Помощник прокурора района Шумакова М.В.