**Об ответственности за мошенничество в сфере компьютерной информации**

В Российской Федерации последние годы отмечается существенный рост преступлений в сфере компьютерной информации и деяний, совершенных с использованием информационных технологий. Преступники достаточно часто осуществляют неправомерное воздействие на абонентские базы данных операторов мобильной связи, интернет-провайдеров либо банковские или служебные базы данных, нарушая правила эксплуатации информационных систем, правила доступа к информационным системам, что влечет причинение вреда критической информационной инфраструктуре Российской Федерации.

Ответственность за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации предусмотрена ст. 274.1 УК РФ и содержит несколько самостоятельных форм преступного посягательства, а именно:

-создание, распространение, использование вредоносных компьютерных программ влечет лишение свободы от двух до пяти лет со штрафом;

-неправомерный доступ к компьютерной информации наказывается лишением свободы на срок от двух до шести лет со штрафом;

-нарушение правил эксплуатации средств хранения, обработки или передачи информации, которые посягают на общественные отношения в сфере безопасного функционирования компьютерной информации, средств хранения, обработки или передачи такой информации влечет лишение свободы на срок до шести лет.

Возможно лишение права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет. Более суровое наказание предусмотрено, если деяния повлекли тяжкие последствия.

При этом стоит отметить, что преступления, совершаемые с использованием информационно-телекоммуникационных технологий, имеют ряд особенностей:

1. не происходит физического контакта между злоумышленником и жертвой;
2. большинство следов данного рода преступлений носит "цифровой" характер, используются специальные программы, в том числе и программы на основе искусственного интеллекта (например, использование чат-ботов для разработки и проведения фишинговых кампаний, обнаружения и использования уязвимости, проведения хакерских атак, создания и распространения вредоносных программ);
3. при совершении таких преступлений злоумышленниками учитывается и эксплуатируется особенность человеческого характера;
4. преступления и правонарушения, носят латентный характер, так как пострадавшие не обращаются с заявлениями в правоохранительные органы;
5. эти преступления совершаются, как правило, по определенным схемам, однако эти схемы систематически видоизменяются;
6. отсутствуют территориальные ограничения в совершении данного вида преступлений.

Специфика этого преступления заключается в том, что обман перенесен в виртуальный мир, в сферу компьютерной информации и заключается в совершении следующих неправомерных действий (операций), который приводит к хищению чужого имущества или приобретению права на чужое имущество:

-ввод сфальсифицированной компьютерной информации;

-удаление действительной компьютерной информации, при котором уничтожаются реальные данные (например: о реальном владельце акций, земельного участка и др.) или же они искажаются в результате того, что оставшаяся информация не является полной;

-блокировка компьютерной информации, т.е. информация продолжает существовать, но становится недоступной для пользователей;

-модификация (искажение) компьютерной информации;

-иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно- телекоммуникационных сетей.

Прокуратура Токаревского района