П Р О К У Р А Т У Р А

города Нижневартовска

Киберпреступления, установленная законом ответственность за их совершение и способы предотвращения

Киберпреступление — это общее название для всех типов криминальной активности, совершаемой с использованием вычислительных машин и/или Интернета. Киберпреступление может совершаться с помощью различных методов и инструментов, например, фишинг, вирусы, шпионское программное обеспечение, программы-вымогатели и социальная инженерия — чаще всего с целью кражи личных данных или финансовых средств.

Киберпреступность в Российской Федерации на сегодняшний день достигла большого размаха, чему чрезвычайно поспособствовало повсеместное подключение граждан к информационно-телекоммуникационная сети «Интернет» с помощью ноутбуков, смартфонов, планшетов и других устройств, и по праву считается одной из самых прибыльных сфер криминального бизнеса в целом.

Рассмотрим некоторые распространенные виды киберпреступлений. Одним из них является кибермошенничество, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.).

Наиболее распространенным видом кибермошенничества является так называемый «скимминг». Его суть заключается в том, что с помощью технических средств преступники копируют магнитную полосу карты и считывают ее пин-код. На основе полученных данных они изготавливают поддельную пластиковую карту, при использовании которой деньги списываются с оригинала.

Другой способ кибермошенничества – «фишинг», когда преступники получают информацию о карте дистанционно. Для этого они присылают гражданину SMS с просьбой сообщить пин-код и cvv-код, представляясь сотрудниками банка.

В целях противодействия развитию и росту киберпреступности, федеральным законодателем установлена юридическая ответственность за совершение данного рода деяний.

Согласно ч. 1 ст. 159.6 Уголовного кодекса Российской Федерации под мошенничеством в сфере компьютерной информации понимается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного

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

За данное преступление предусмотрена уголовная ответственность в виде штрафа в размере до 120 тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательные работы на срок до 360 часов, либо исправительные работы на срок до одного года, либо ограничение свободы на срок до двух лет, либо принудительные работы на срок до двух лет, либо арест на срок до четырех месяцев.

Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. ст. 272, 273 или 274.1 Уголовного кодекса Российской Федерации.

Согласно ч. 1 ст. 159.3 Уголовного кодекса Российской Федерации под мошенничеством с использованием платежных карт понимается хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации.

Указанное деяние наказывается штрафом в размере до 120 тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до 360 часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на срок до трех лет.

Уголовно-наказуемым деянием является изготовление, приобретение, хранение, транспортировка в целях использования или сбыта поддельных платежных карт, а также сбыт поддельных платежных карт. Также законом установлена ответственность за изготовление, приобретение, хранение, транспортировку в целях использования или сбыта электронных средств, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств.

Противодействие киберпреступлениям относится к компетенции правоохранительных органов, уполномоченных на обеспечение информационной безопасности. Вместе с тем, рядовые пользователи также могут существенно поспособствовать пресечению роста киберпреступности, заблокировав основной метод распространения киберпреступлений: вредоносное программное обеспечение.

Также, в целях предупреждения киберпреступлений пользователям следует придерживаться следующих мер информационной безопасности: не загружать файлы из непроверенных источников; не переходить по ссылкам, содержащимся в электронных письмах незнакомых отправителей; не сообщать никому свои пароли и личные данные.

Одним из наиболее эффективных методов защиты персональных данных, содержащихся на компьютерных и мобильных устройствах, от несанкционированного доступа киберпреступников по-прежнему является использование современных и качественных антивирусных программ.

О ставших известными фактах совершения киберпреступлений, следует незамедлительно сообщить в органы внутренних дел.

Пресс-служба
Прокуратуры г. Нижневартовска