Ответственность за совершение преступлений в сфере компьютерной информации

Компьютерные преступления в России уже давно перестали быть редкостью. С каждым годом незаконных действий с использованием компьютерного оборудования становится все больше и больше.

Такие преступления тесно связаны с нарушением авторских прав. Каждая программа, созданная для той или иной модели ЭВМ (антивирус, драйверы) – продукт автора, владельца. Копирование и продажа дисков с этими программами, взлом защиты с целью завладеть идентификационным ключом – действия незаконные. Во многих случаях киберпреступники взламывают чужие страницы социальных сетей, такие действия являются нарушением частных прав: на личную жизнь, переписку и т.д. Часто потерпевший по таким делам может находиться в одном регионе РФ, а преступник – в другом, в том числе и за границей. Уголовный закон предусматривает ответственность за такие деяния по ст. 137, 138 УК РФ. В последнее время значительно возросло число случаев мошенничества с использованием сети «Интренет».

Многие из нас сталкиваются с противозаконным списанием денег с кредитных карт, виртуальных счетов, оплатой покупок в сети от имени другого лица и т.д. Когда это связано с несанкционированным доступом к различным программам, действия подпадают под признаки уголовных преступлений, которые посягают на безопасность компьютерной информации. Незаконные посягательства на информационную безопасность можно условно разделить на два вида: противозаконные действия в отношении материальных носителей информации (заражение вирусом компьютера, приведение в негодность дисков или незаконное их копирование и т.д.); противозаконные действия по использованию самой информации (похищение конфиденциальных баз данных, уничтожение важной информации или сбыт личной информации, полученной в результате неправомерного доступа). Чаще всего такие преступления совершаются с использованием сети Интернет.

Ответственность за преступления в сфере компьютерной информации предусмотрена в главе 28 Уголовного Кодекса РФ.

1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) Это один из часто встречающихся видов преступления в киберсфере. Информация, доступ к которой запрещен посторонним, может составлять государственную, банковскую, врачебную, служебную или иную тайну. Для невозможности посторонним лицам воспользоваться сведениями устанавливается специальная защита, особое программное обеспечение, система паролей и кодов. Несанкционированный доступ (то есть, получение возможности как минимум ознакомления) к любой охраняемой информации на компьютерах или носителях может стать основанием для привлечения в качестве обвиняемого, если это повлекло: уничтожение данных (приведение

системы в состояние, которое исключает ее использование по назначению); блокировку (становится невозможным правомерный доступ к программе); модификацию (внесение изменений в программу, в текст с информацией и др.); копирование охраняемой информации (на любые носители: бумажный, флеш-карту и т.д.).

2.Создание использование и распространение вредоносных компьютерных программ вредоносных программ (ст. 273 УК РФ) Такой вид преступления в сфере компьютерной информации тоже распространен, есть множество примеров уголовных дел. Речь идет о намеренном создании таких компьютерных продуктов (программ, комбинаций), с помощью которых можно: блокировать; уничтожить; модифицировать; копировать информацию, безопасность которой охраняется. Кроме того, создатель таких вредоносных программ может преследовать цель отключения защиты, которая специально установлена в целях обеспечения безопасности тех или иных сведений. Примерами таких программ могут быть вирусные «черви», троян, кейлоггеры, вирус-сканеры и т.д. Их создание может быть выражено не только в изготовлении и полной подготовке к работе, но и в чертеже схемы, на основе которой предполагается использовать вредоносные системы, а также в написании алгоритма, при введении которого наступит одно из последствий, указанное выше.

3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) Данный вид преступления может быть и бездействием. В ст. 274 УК РФ предусмотрена ответственность должностных лиц, на которые возложены обязанности по правильному: хранению; эксплуатации (использованию); обработки; передачи компьютерной информации. В статье не отражены требования, которые должны быть соблюдены теми или иными должностными лицами. В каждом конкретном деле нужно обращаться к федеральным законам, должностным инструкциям, уставам, в которых подробно указан порядок обращения с информацией. Примерами ненадлежащего хранения, обработки компьютерной информации могут быть уголовные дела в отношении сотрудников избиркома, оборонной промышленности, организаций телефонной и интернет-связи, неправильно использующих закрытые для общего доступа сведения и т.д.

4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст.274.1 УК РФ), Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2 УК РФ). Данные составы преступлений подразумевают угрозу безопасности государства и населения.