УДК 343.97

Е. И. Шайтарова

ОТВЕТСТВЕННОСТЬ ЗА РАЗРАБОТКУ, ИСПОЛЬЗОВАНИЕ ЛИБО РАСПРОСТРАНЕНИЕ ВРЕДОНОСНЫХ ПРОГРАММ ПО БЕЛОРУССКОМУ ЗАКОНОДАТЕЛЬСТВУ

За последние несколько лет интернет стал опасным местом. Изначально созданный для сравнительно небольшого количества пользователей, он значительно превзошел ожидания своих создателей. Сегодня в мире насчитывается более 1,5 миллиардов интернет-пользователей и их число постоянно растет по мере того, как технология становится все более доступной.

Преступники тоже заметили эту тенденцию и очень быстро поняли, что совершение преступлений с помощью интернета (теперь это получило название киберпреступления) имеет ряд существенных преимуществ.

Государственные органы, физические и юридические лица вправе осуществлять поиск, получение, передачу, сбор, обработку, накопление, хранение, распространение и (или) предоставление информации, пользование информацией в соответствии с законодательством.

Уголовный кодекс Республики Беларусь (ст. 354) предусматривает уголовную ответственность за разработку, использование либо распространение вредоносных программ.

Предметом данного преступления являются: компьютерные программы, не-санкционированно уничтожающие, блокирующие, модифицирующие или копиру-ющие компьютерную информацию; специальные вирусные программы; носители с вредоносными программами. Определение «вредоносная программа» дано на международном уровне – в ст. 1 Соглашения о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации. Под вредоносной программой в этом Соглашении понимается «созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети».

Необходимо разъяснить исходя из диспозиции данной статьи в чем заключается, каждое из вышеперечисленных действий:

1) разработка вредоносных программ, равно как и разработка специальных ви-русных программ заключается в написании их алгоритма, т. е. последовательнос-ти логических команд, дальнейшего преобразования текста в машиночитаемую форму с последующим введением его в ЭВМ или без такового;

2) внесение изменений в существующие программы означает изменение их алгоритма путем исключения из текста отдельных фрагментов, замены их

другими, дополнения его новыми фрагментами и пр., в результате чего программы приобретают свойство несанкционированно уничтожать, блокировать, модифи-цировать или копировать компьютерную информацию;

3) заведомое использование вредоносных компьютерных либо специальных вирусных программ подразумевает сознательное их применение при эксплуатации ЭВМ и обработке информации;

4) распространение носителей с вредоносными компьютерными либо специальными вирусными программами состоит в передаче носителей с такими програм-мами третьим лицам как за плату, так и бесплатно, как в постоянное владение, так и временно, а равно в предоставлении доступа к компьютерной информации, воспроизведенной в любой материальной форме, в том числе сетевым или иным способами.

Проблема вредоносных программ – рекламных и шпионских – заслуживает повышенного внимания как одна из самых главных неприятностей, с которыми ежедневно сталкиваются современные пользователи компьютеров. Необходимо комплексное понимание проблемы киберпреступности, всесторонне взаимодействие не только правоохранительных органов, но и производителей технико-программных продуктов и средств.

Наиболее опасную категорию вирусописателей составляют хакеры-одиночки или группы хакеров, которые осознанно или неосознанно создают вредоносные программы с единственной целью: получить чужие деньги (рекламируя что-либо или просто воруя их), ресурсы зараженного компьютера. Обслуживание рекламного и спам-бизнеса – один из основных видов деятельности таких хакеров.

Вторым видом деятельности подобных вирусописателей является создание, распространение и обслуживание троянских программ-шпионов, направленных на воровство денежных средств с персональных «электронных кошельков» или с обслуживаемых через интернет банковских счетов. Троянские программы данного типа собирают информацию о кодах доступа к счетам и пересылают ее своему «хозяину».

Третьим видом криминальной деятельности этой группы является интернет-рэкет, то есть организация атаки на один или несколько интернет-ресурсов с последующим требованием денежного вознаграждения за прекращение атаки. Обычно под удар попадают интернет-магазины, букмекерские конторы.

На сегодняшний день наблюдается устойчивая тенденция роста числа компьютерных преступлений на фоне незначительного количества выявленных и привлеченных к ответственности за указанные деяния лиц. Это дает веские основания для вывода о недостаточности теоретико-правового обеспечения основ практической деятельности по устранению причин и усло-

вий совершения данного вида преступлений, их эффективному предупреждению.

Ущерб компьютерной информации, наносимый сегодня вредоносными программами, представляет собой одну из наиболее существенных угроз конституционным правам и свободам граждан, а также экономической и общественной безопасности государства, поскольку, нарушая информационные правоотношения субъектов, он тем самым ставит под сомнение саму возможность нормального функционирования государственных и общественных институтов.