

Лебедев А.С., Сошина И.М.

Студент, ФГБОУ ВО ЛГПУ имени П.П. Семенова-Тян-Шанского, (г. Липецк)

Студент, ФГБОУ ВО ЛГПУ имени П.П. Семенова-Тян-Шанского, (г. Липецк)

Lebedev A. S., Soshina I. M.

Student, «Lipetsk State Pedagogical P. Semenov-Tyan-Shansky University»

Student, «Lipetsk State Pedagogical P. Semenov-Tyan-Shansky University»

УГОЛОВНО-ПРАВОВАЯ ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ

Аннотация

Данная статья посвящена проблеме уголовно-правовая ответственность за преступления в информационной сфере. В статье рассматриваются основные законы уголовно-правовая ответственность за преступления в информационной сфере.

Ключевые слова: информация, безопасность, уголовная ответственность.

Criminal liability for crimes in the information sphere

Annotation

This article is devoted to the problem of criminal liability for crimes in the information sphere. The article deals with the basic laws of criminal liability for crimes in the information sphere.

Keywords: information, security, criminal liability.

«Информационная революция» застала Россию в сложный экономический и политический период. Необходимость досрочной разработки правовых основ охраны информационных отношений, еще слабая развитость электронно-вычислительных систем, незначительное количество выявленных общественно опасных посягательств на эти отношения, отсутствие необходимого опыта привело к тому, что во вновь принятом в 1996 года Уголовном кодексе РФ в гл. 28 «Преступления в сфере компьютерной информации» содержалось три статьи, предусматривающие ответственность за «Неправомерный доступ к компьютерной информации» (ст. 272), «Создание, использование и распространение вредоносных

программ для ЭВМ» (ст. 273) и «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274). Названные в ст. 272 и 274 УК РФ деяния относятся к преступлениям небольшой тяжести, а эти же преступления, совершенные при отягчающих обстоятельствах, – к преступлениям средней тяжести [1].

В тот период времени эти нормы в минимальной степени удовлетворяли потребности правоприменительной практики. В настоящее время с компьютеризацией общества, переходом на расчеты финансовых и банковских структур с использованием электронно-вычислительных машин и в связи с транснациональным характером компьютерной преступности упомянутые нормы не могут обеспечить борьбу с компьютерными преступлениями. В них не учтено многообразие общественных отношений, на которые посягают названные преступления (это не только экономические интересы, но и государственная безопасность, конституционные права человека, его честь и достоинство т.д.).

Несмотря на новизну компьютерных преступлений для отечественного уголовного законодательства, в государствах с высоким уровнем технологического развития проблема с компьютерной преступностью давно признана одной из первостепенных задач, важность которой неуклонно возрастает.

Недооценка общественной опасности посягательств на интересы, охраняемые гл. 28 УК РФ, в сочетании с конструктивными недостатками диспозиций этих уголовно-правовых норм, а также недостаточным уровнем подготовки правоприменительных органов, призванных вести борьбу с компьютерными преступлениями, привели к тому, что уголовно-правовые нормы, предусматривающие ответственность за названные преступления, применяются очень редко [2].

Сложившееся положение объясняется рядом причин, среди которых в первую очередь представляется необходимым выделить:

а) недостаточную разработанность теоретической модели компьютерных преступлений;

б) недостаточную изученность криминологической характеристики компьютерных преступлений и в этой связи неразработанность более совершенных методик по раскрытию и расследованию преступлений, комплекса мер предупредительного характера и рекомендаций по виктимологической профилактике.

Необходимость разработки новой системы компьютерных преступлений возникает еще и потому, что в ст. 272 – 274 УК РФ совершенно не учтены общественно опасные последствия неправомерного доступа в чужую компьютерную информацию.

Если в результате преступления причиняется ущерб, содеянное квалифицируется по статьям о преступлениях против собственности [3].

Представляется, что уголовно-правовые нормы об ответственности за преступления, совершенные с использованием высоких технологий, лицами, обладающими большим интеллектуальным потенциалом, влекущие тяжелые последствия, должны предусматривать более строгое наказание, чем обычные преступления против собственности. При построении системы компьютерных преступлений следует учесть опыт зарубежных государств, где компьютерная преступность оказалась более распространенной и нанесла более серьезный ущерб.

Список используемой литературы:

1. Абов А.И., Ткаченко С.Н. Международный и отечественный опыт борьбы с компьютерными преступлениями. – М., 2004. – С. 5–28.
2. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. – М., 2005. – 611 с.
3. Гурьянов К.В. Файлы CRACK как идентификационный признак совершения преступлений в сфере производства компьютерного

(информационного) контрафакта // Эксперт-криминалист. – 2007. – № 3. – С. 12-20.