

## **Правонарушения в сфере информационных технологий**

**Петрухина Т.А., Хорсуненко К.И.**

В Российской Федерации развитие и эффективное использование информационных технологий (ИТ) является одним из приоритетных направлений государственной политики. Целью формирования и развития информационного общества в Российской Федерации являются повышение качества жизни граждан, обеспечение конкурентоспособности России, развитие экономической, социально-политической, культурной и духовной сфер жизни общества, совершенствование системы государственного управления на основе использования информационных и телекоммуникационных технологий.

Информационные технологии (ИТ) стали одним из ведущих факторов прогресса цивилизации. Информационные технологии, наряду с телекоммуникационными технологиями, составляют основу процессов информатизации, движения к информационному обществу.

"Информационная революция" застигла Россию в сложный экономический и политический период и потребовала срочного регулирования возникающих на ее пути проблем. Необходимость разработки юридических основ информационных отношений привела к поспешному и не всегда корректному формированию ряда базовых правовых понятий в этой области с их уточнением в каждом следующем нормативном акте.

Современные информационные системы составляют техническую основу органов управления государственной власти, промышленных предприятий и научно-исследовательских организаций, учреждений кредитно-финансовой сферы, банков и т.п. Разработка новейших технологий влечет за собой поступательное развитие новых средств коммуникации, рост их производства и модификации, создавая новые пласты собственности, бизнеса.

Сейчас, когда создан и принят ряд базовых нормативных актов в области информационных отношений, наступило время для их применения на практике.

Однако на этом пути неизбежны пробы и ошибки. Проблема информационной безопасности возникла достаточно давно. До сравнительно недавнего времени методы защиты информации были в исключительной компетенции спецслужб, обеспечивающих безопасность

страны. Однако новые технологии измерения, передачи, обработки и хранения информации значительно расширили сферы деятельности людей, нуждающихся в защите информации, привели к развитию и распространению новых методов несанкционированного доступа к информации и, как следствие, к интенсивному развитию нового научного направления - «информационная безопасность».

Преступления в сфере информационных технологий включают как распространение вредоносных вирусов, взлом паролей, кражу номеров банковских карт и других банковских реквизитов (фишинг), так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду), а также вредоносное вмешательство через компьютерные сети в работу различных систем. Кроме того, одним из наиболее опасных и распространенных преступлений, совершаемых с использованием Интернета, является мошенничество.

Необходимо также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надёжности функционирования информационных систем.

Стремительное развитие информационных и коммуникационных технологий, а также компьютеризация мирового сообщества вообще, вызвало острую необходимость включения в правовую систему Российской Федерации юридических норм, которые бы регулировали правоотношения возникающие в сфере сбора, обработки, накопления (хранения) и передачи информации, а также использование компьютерной техники, средств хранения информации (носителей информации) и каналов связи (телекоммуникаций).

Преступность сегодня стала одним из основных дестабилизирующих факторов развития нашего общества. Ее масштабы представляют реальную угрозу процессу становления российской государственности, успешному осуществлению социально-экономических реформ.

Российским специалистам, входящим в состав отечественных организованных преступных групп и сообществ, осуществляющих свою преступную деятельность, в настоящее время не составляет большого

труда "взломать" многие системы защиты информации и получить доступ к сведениям, составляющим государственную или коммерческую тайну.

К сожалению, нормой сегодняшнего времени стала кража компьютерного программного обеспечения, которая осуществляется путем нелегального копирования и дальнейшего тиражирования лицензионных программных продуктов. Программное пиратство считается наиболее общим и наиболее "дорогим" типом компьютерного преступления.

Не случайно защита данных в компьютерных сетях, борьба с компьютерной преступностью становится одной из актуальных проблем российского уголовного законодательства.

В настоящее время под компьютерными преступлениями подразумеваются: неправомерный доступ к компьютерной информации (статья 272 УК РФ); создание, использование и распространение вредоносных программ (статья 273 УК РФ); нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (ст. 274 УК РФ).

К правовым мерам следует отнести разработку правовых норм, устанавливающих уголовную ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. Несмотря на значимость информации, как объекта уголовно-правовой защиты, в современном российском уголовном законодательстве, а также в теории уголовного права не существует системного подхода к данной проблеме. В уголовном законодательстве самостоятельно обозначены лишь преступления в сфере компьютерной информации.

Представители правоохранительных органов испытывают затруднения при квалификации преступлений в сфере компьютерной информации. Это объясняется рядом причин:

- 1) это недостаточная проработка действующего законодательства, а также следственной и судебной практики привлечения к уголовной ответственности за компьютерные преступления;
- 2) трудности доказывания и судебных исследований, связанных с использованием нетрадиционных носителей информации, недостаточная изученность и практика этого объекта права;
- 3) криминалистические проблемы, состоящие в том, что технико-криминалистические, тактические и методические приёмы, методы и средства раскрытия и расследования подобного рода преступлений в

полной мере не отработаны как на теоретическом, так и на практическом уровнях;

4) сложности организационного характера, состоящие в том, что при относительном насыщении аппаратными и техническими средствами правоохранительные органы до сих пор не имеют развитой системы локальных сетей, достаточного количества квалифицированных специалистов по использованию таких средств для целей расследования.

В связи с бурным процессом развития научно-технической революции сформировался новый вид общественных отношений - информационные. Информационные отношения стали новым объектом, а информация - новым предметом преступного посягательства. Неизбежным следствием появления новых общественных отношений стали правонарушения в сфере компьютерной информации, в том числе и в форме преступлений, которые представляют реальную угрозу для нормального развития и течения общественной жизни.

Преступления в сфере компьютерной информации можно определить как умышленные общественно опасные деяния, причиняющие вред либо создающие угрозу причинения вреда общественным отношениям, регламентирующим безопасное производственное хранение, использование или распространение информации и информационных ресурсов либо их защиту.

Видовым объектом преступлений в сфере компьютерной информации являются информационные отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

Таким образом, можно сделать вывод, что существует необходимость совершенствования уголовно-правовой защиты компьютерной информации в связи с постоянно возрастающим значением и широким применением ЭВМ во многих сферах деятельности и наряду с этим повышенной уязвимостью компьютерной информации.