**Социальная опасность правонарушений в сфере новых информационных технологий**

Юренков О.Г.

Научно-техническая революция, свидетелями которой мы являемся, повлекла за собой серьезные социальные изменения, наиболее важным из которых является появление нового вида общественных отношений и общественных ресурсов - информационных.

Информация стала первоосновой жизни современного общества, предметом и продуктом его деятельности, а процесс ее создания, накопления, хранения, передачи и обработки в свою очередь стимулировал прогресс в области орудий ее производства: электронно-вычислительной техники, средств телекоммуникаций и систем связи. Следствием протекающих в обществе информационных процессов является возникновение и формирование новых социальных отношений и изменение уже существующих.

Однако новые информационные технологии дали толчок не только прогрессу общества, но и стимулировали возникновение и развитие неизвестных ранее негативных процессов. Одним из них является появление новых видов правонарушений.

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. Набирают силу опасные процессы сращивания традиционной преступности с так называемой "беловоротничковой" - экономической и компьютерной. Российским специалистам, входящим в состав отечественных организованных преступных групп и сообществ, осуществляющих свою преступную деятельность в том числе и на территориях США и Западной Европы, в настоящее время не составляет большого труда "взломать" многие системы защиты информации и получить доступ к сведениям, составляющим государственную или коммерческую тайну.

Также, одним из негативных социальных последствий развивающегося научно-технического прогресса является изменение характера преступлений и способов их совершения:

ћ возросли динамизм совершаемых преступлений, мобильность и техническая оснащенность преступников. Для подготовки и совершения противоправных действий организованные преступные группы применяют средства радиосвязи (радиостанции, средства пейджинговой, транкинговой, сотовой и даже космической связи), навигации, электронно-вычислительные машины (ЭВМ), технические средства радиомониторинга, а также некоторые оперативно-технические средства;

ћ появились новые виды преступлений - использование ЭВМ для присвоения собственности, кража математического обеспечения и программ из автоматизированных систем, шантаж с помощью ЭВМ и др.;

ћ организованные преступные группы используют в своей деятельности новейшие достижения науки и техники - применяют системный подход при планировании операций; разрабатывают оптимальные варианты их проведения и обеспечения; создают системы электронного слежения и наблюдения.

Особо важной задача обеспечения информационной безопасности является для органов государственной власти, т.к., условно, на абстрактном уровне, работу государственного служащего можно определить как непрерывный процесс сбора, обработки, анализа и передачи информации различной категории важности с точки зрения обеспечения ее защиты. Необходима разработка действенной системы практических мер обеспечения информационной безопасности при обработке данных с использованием вычислительной техники и средств передачи данных. И если система мер защиты данных при работе на отдельной ПЭВМ достаточно хорошо проработана и регламентирована, то этого нельзя сказать для внедряемых в деятельность органов государственной власти распределенных систем обработки и передачи данных (локальные вычислительные сети, региональные и ведомственные системы, сети общего пользования).

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. Так, по оценкам различных юридических служб, ущерб от деятельности интеллектуальных пиратов в 1997 году составил в целом по стране более одного миллиарда долларов США. По мнению МВД России сегодня это явление принимает угрожающий характер в России.

Правонарушения в сфере новых информационных технологий можно определить, как все противоправные и социально-вредные формы поведения, которые осуществляются с использованием средств вычислительной техники, средств телекоммуникаций и систем связи. Большая часть противоправных форм поведения, характерных для применения вычислительной техники, направлена на то, чтобы нанести ущерб имуществу, которое зависит от данных, хранящихся в памяти ЭВМ.

ЭВМ является самым многообещающим орудием преступления в будущем. Уже сейчас экономический ущерб от преступлений, совершаемых с помощью ЭВМ, в развитых странах сопоставим с преимуществами от их внедрения, а социальные, моральные потери вообще не поддаются оценке. В деловом обзоре Американской ассоциации адвокатов указывается, что почти половина преступлений в деловом мире связана с использованием компьютеров. Согласно данным специального доклада Института компьютерной безопасности, расположенного в Сан-Франциско (штат Калифорния), в 1997 году в США число компьютерных преступлений увеличилось на 16 процентов по сравнению с 1996 годом. Доклад построен на результатах опроса руководителей 520 государственных и общественных организаций, а также частных фирм США, которые сообщили, что их убытки от этих видов преступлений в истекшем году составили 136 миллиардов долларов США Появились профессиональные "компьютерные преступники" и в нашей стране (известный пример - "хакер" Левин).

Совершенно очевидно, что борьба с подобными проявлениями требует предварительного изучения социальных факторов, способствующих совершению данных правонарушений, разработки адекватных научных методов, более совершенных технических средств раскрытия и расследования, проведения специальных оперативно-розыскных и оперативно-технических мероприятий и т.д. Для обеспечения действенной борьбы с преступностью в условиях развития научно-технического прогресса должны использоваться методы и средства, обладающие по крайней мере не меньшей эффективностью, чем те, которые применяют в свой деятельности организованные преступные группы.

С учетом широкого распространения правонарушений в сфере новых информационных технологий в развитых странах, значительного опыта борьбы с этими явлениями на Западе, важно правильно использовать материалы зарубежного опыта в этой новой для нас сфере правоохранительной деятельности.