На основе анализа совершаемых преступлений в сфере компьютерной информации и с использованием ЭВМ, системы и сети ЭВМ и научных точек зрения на новый вид преступности в современном мировом сообществе и в России, предлагается определение преступности в сфере высоких технологий.

Современный этап развития мирового сообщества характеризуется стремительным развитием научнотехнического прогресса, в который включается и сфера высоких технологий. В Окинавской хартии глобального информационного общества отмечалось, что «...информационные телекоммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества XXI в. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. Информационнокоммуникационные технологии быстро становятся важным стимулом развития мирового общества» [7. С. 52]. Вместе с тем развитие научно-технического прогресса всегда сопровождается всплеском негативных общественных проявлений, в частности таких, как преступность.

Указанные обстоятельства предопределили появление новой разновидности преступности, которая в российских и зарубежных научных источниках получила названия «киберпреступность», «электронная преступность», «преступность в сфере высоких технологий», «компьютерная преступность».

В отечественной юридической литературе даются неоднозначные определения преступности в рассматриваемой сфере общественных отношений. Так, З.И. Кирсанов определяет компьютерную преступность как совокупность преступлений в сфере компьютерной информации:

а) неправомерный доступ к охраняемой законом информации, повлекший уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети; б) создание, использование и распространение вредоносных программ для ЭВМ, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, их систем или сетей; в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование

или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред [10. С. 258].

На наш взгляд, указанное определение не охватывает всего спектра преступлений, совершаемых с использованием ЭВМ, системы и сети ЭВМ и новейших информационных технологий. Представляется, что данное явление следует рассматривать как преступность в сфере компьютерной информации, поскольку автор указывает только преступления в сфере компьютерной информации, предусмотренные в гл. 28 Уголовного Кодекса Российской Федерации (ст. 272, 273, 274).

Имеют место и другие определения данного вида преступности. Так, А.И. Долгова справедливо отмеча-

ет, что компьютерная преступность - сравнительно новое и многозначно толкуемое понятие. Наиболее распространенными являются следующие определения:

1) совокупность преступлений в сфере компьютерной информации (в УК РФ данные преступления предусмотрены в гл. 28); 2) совокупность преступлений, совершаемых с использованием компьютера. Автор отмечает, что германские ученые выделяют такие характерные признаки компьютерной преступности, как использование компьютера в качестве средства или объекта совершения преступления. За рубежом активно обсуждается вопрос, стоит ли относить к компьютерным преступлениям и другие преступления, связанные с компьютером, но не затрагивающие имущественный интерес: вторжение в сферу личной, семейной тайны и т.п. По мнению А.И. Долговой, исследователю, оперирующему термином «компьютерная преступность», следует конкретизировать исходное понятие [10.

С. 590-591].

Проблемы и тенденции преступности в сфере высоких технологий и пути уголовно-правового противодействия ей рассматривались в научных трудах Ю.М. Батурина, И.Л. Бачило, В.Б. Вехова, А.Г. Волеводза, В.А. Копылова, В.В. Крылова, В.В. Лунеева, В.Н. Лопатина, Ю.И. Ляпунова, Э.Ф. Побегайло, С.А. Яни и ряда других авторов. Однако стремительное развитие данной сферы, появление новых видов преступлений, совершаемых с помощью ЭВМ, системы, сети ЭВМ и новейших технологий, требуют более глубокого и всестороннего изучения проблемы; в современных условиях она перестала быть национальной проблемой отдельно взятого государства и превратилась в транснациональную проблему всего

мирового сообщества.

Наиболее распространенные преступления в рассматриваемой сфере - неправомерный доступ к охраняемой законом компьютерной информации; создание, использование и распространение вредоносных программ для ЭВМ. Общее количество зарегистрированных преступлений в сфере компьютерной информации, по данным МВД РФ, составило: в 1997 г. - 7; в 1998 г. - 66; в 1999 г. - 294; в 2000 г. - 800; в 2001 г. -2086; в 2002 г. - 4122; в 2003 г. - 7782; в 2004 г. количество преступлений увеличилось почти в два раза, и на сегодняшний день тенденция роста сохраняется. При этом отмечаются устойчивый рост числа преступлений, предусмотренных ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» (1997 г. - 6; 1998 г. - 53; 1999 г. - 209; 2000 г. - 584; 2001 г. - 1619; 2002 г. - 3782; 2003 г. - 7053), и тенденция снижения количества преступлений, предусмотренных ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» (1997 г. - 0; 1998 г. - 1; 1999 г. - 0; 2000 г. - 44; 2001 г. - 120; 2002 г. - 10; 2003 г. - 1).

С развитием компьютерной техники появилась и преступность, связанная с электронной обработкой информации. Один из самых опасных видов этой преступности, получивший наибольшее распространение в последнее время, - хакинг. Хакеры взламывают защиту компьютерных сетей, отключают сайты учреждений и компаний, «нападают» на серверы банков, фирм, организаций, имеющих стратегическое значение.

Сегодня Интернет можно рассматривать как оружие террористов. По мнению специалистов, терроризм с использованием последних достижений в сфере высоких технологий не менее опасен, чем бактериологический или ядерный.

Арсенал компьютерных террористов - различные вирусы, логические бомбы (команды, встроенные заранее в программу и срабатывающие в нужный момент). Современные террористы используют Интернет в основном как средство пропаганды, передачи информации, а не как новое оружие. Однако можно предполагать, что компьютерный терроризм сегодня уже не фантазия, а реальность. В настоящее время существует мало систем, которые можно назвать абсолютно защищенными.

В связи с тем, что компьютерный терроризм уже представляет собой реальность, необходимо закрепить на законодательном уровне обязанность государственных структур по принятию технических, правовых и организационных мер,

обеспечивающих защиту компьютерных сетей как одного из уязвимых элементов современного российского общества.

В российской юридической литературе проблемы компьютерного терроризма, его определение освещены весьма слабо и трактуются неоднозначно.