

## **ПРЕСТУПЛЕНИЯ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ: УГОЛОВНО – ПРАВОВАЯ ХАРАКТЕРИСТИКА И АКТУАЛЬНЫЕ ПРОБЛЕМЫ**

*В.Г. Пирва*

Юридический институт Байкальского государственного  
университета, г. Иркутск

В современном мире компьютерная информация внедрилась во все сферы жизни общества. Вместе с этим возник ряд острых проблем [1] и негативных проявлений. В юридической литературе неоднозначно определяют эти сферы: компьютерная преступность, киберпреступность, преступность в сфере высоких технологий и т.п. Дискуссионным вопросом остается определение понятия «компьютерная преступность» и «преступления в сфере высоких технологий».

К.Р.Абызов, В.Г.Гриб, И.С.Ильин определяют «компьютерную преступность» как совокупность компьютерных преступлений, где компьютерная информация является предметом преступных посягательств, а также преступлений, которые совершаются посредством общественно опасных деяний, предметом которых является компьютерная информация[2]. В то же время такие ученые как В. П. Ревина и А. И. Рарог трактуют понятие «компьютерная преступность» через призму Российского уголовного закона как виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства[3]. Вышеуказанное определение, на наш взгляд, с учетом развития компьютерных и иных технологий является более точным и актуальным на сегодняшний день.

Некоторые авторы, в том числе З.И. Кирсанов, относят к компьютерной преступности следующее: 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[4]. Анализируя данное мнение, можно сказать, что оно является слишком узким, поскольку охватывает только те преступления, которые закреплены в Главе 28: «Преступления в сфере компьютерной информации» Уголовного кодекса Российской Федерации.

По мнению А.И. Долговой, компьютерной преступностью следует считать, помимо вышеуказанного, и совокупность преступлений, совершаемых с использованием компьютера[5]. Таким образом, соглашаясь с А. И. Долговой и К. И. Поповым, что компьютерные преступления - это любое противоправное действие, при котором ЭВМ выступает либо как объект, против которого совершается преступление, либо как инструмент, используемый для совершения преступных действий[6].

Законодатель выделил в отдельную Главу 28 «Преступления в сфере компьютерной информации», этим разделил современную технику и технологии. Из этого следует, что результатом формирования и развития системы технологий приходит именно от информационных систем и стандартизации. В современном законодательстве России легальное определение понятия «Высокие технологии» также отсутствует, хотя имеет собирательный характер.

В доктрине уголовного права под исследуемым определением понимают новые и прогрессивные современные изобретения, в числе которых являются компьютерные, электронно-цифровые технологии, автоматизация и информатизация. В связи с учетом научно - технического прогресса, более логичным будет использования термина «Высокие технологии», который является более широким понятие в отличие от других терминов. К преступлениям в сфере высоких технологий можно отнести следующие:

- 1) Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ);
- 2) Незаконный оборот специальных технических средств, предназначенных для негласного получения информации (ст. 138.1 УК РФ)
- 2) Нарушение авторских и смежных прав (ст. 146 УК РФ);
- 3) Мошенничество с использованием электронных средств платежа (ст.159.3 УК РФ);
- 4) Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);

- 5) Кража с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ) (п. «г» ч. 3 ст. 158 УК РФ)
- 6) Причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ) - при незаконном использовании чужого логина и пароля доступа к ресурсам сети «Интернет»;
- 7) Незаконное предпринимательство (ст. 171 УК РФ);
- 8) Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ);
- 9) Изготовление или сбыт поддельных денег или ценных бумаг (ст. 186 УК РФ);
- 10) Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов (ст. 187 УК РФ);
- 11) Уклонение от уплаты налогов с организаций (ст. 199 УК РФ);
- 12) Незаконное распространение порнографических материалов (ст. 242 УК РФ);
- 13) Изготовление и оборот материалов с порнографическими изображениями несовершеннолетних (ст. 242-1 УК РФ);
- 14) Неправомерный доступ к компьютерной информации (ст. 272 УК РФ);
- 15) Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);
- 16) Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ);
- 17) Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ);
- 18) Подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков (ст. 327 УК РФ).

В связи с этим можно классифицировать объект посяательства в сфере высоких технологий на 4 группы:

1. Компьютерная информация;
2. Сфера экономики;
3. Личные права и неприкосновенность частной жизни;
4. Общественные и государственные интересы.

Анализируя судебную практику, достаточно часто встречаются однотипные преступления в сфере высоких технологий. Примером может служить обвинительный приговор суда от 14.11.2017г. о признании виновным лица в ч. 2 ст. 146 УК РФ и ч.1 ст. 273 УК РФ и назначении наказания в виде ограничения свободы

сроком на 1 (один) год со штрафом в сумме 20000 (двадцать тысяч) рублей. Незаконные действия лица заключались в приобретении из информационно - телекоммуникационной сети «Интернет» методом скачивания программные обеспечения, правообладателями которых являются компании «Microsoft», «Corel» и Графисофт СЕ Европейское частное акционерное общество и вредоносные программные обеспечения в целях извлечения прибыли с использованием технического средства - персонального компьютера. Затем с целью извлечения прибыли, не имея разрешения правообладателей на их распространение и сбыт, разместил в информационно - телекоммуникационной сети «Интернет» на сайте «Avito.ru» объявление о том, что устанавливает и реализует программные обеспечения для персональных электронно - вычислительных машин.

По статистическим данным Генеральной прокуратуры РФ с 2013 по 2016 год число преступлений, совершаемых с использованием высоких технологий в России, увеличилось в шесть раз. Согласно официальной статистики за первое полугодие 2017 г. ущерб составил 1 054 260 000 рублей от преступлений в сфере высоких технологий. Количество преступлений в вышеуказанной сфере за январь - ноябрь 2017 г. составило около 82,4 тыс. Исходя из приведенных статистических данных, можно сделать вывод, что преступления в сфере высоких технологий имеют высокую латентность, которая впоследствии приобретает с каждым годом международный характер. Из вышесказанного следует, что по нынешний день новые высокие технологии продолжают совершенствоваться и развиваться не менее быстрыми темпами, что в свою очередь, создают благоприятную среду для развития преступлений в данной сфере.

Таким образом, необходимо дальнейшее совершенствование Российского уголовного законодательства в сфере высоких технологий, поскольку преступления в вышеуказанной сфере имеет неоднозначный смысл, который достаточно трудно дается оценке по составу преступлений.

### **Библиографический список**

1. Пирва, В.Г., Агильдин, В.В. Мошенничество в сети интернет / В.Г. Пирва / В.В. Агильдин // Современные проблемы правотворчества и правоприменения: матер. Всерос. студен. науч.-практ. конф. / под ред. С.И. Суслова // А.П. Ушакова – Иркутск, 24 марта 2017г. / Иркутск, 2017г. – 312 с.

2. Абызов, К.Р., Гриб, В.Г., Ильин, И.С. Криминология: курс лекций / под ред. В.Г. Гриба. – М.: Маркет ДС, - 2008. – 352 с.
3. Ревина, В.П. Уголовное право России. Особенная часть: учеб. / под ред. В.П. Ревина. - 2-е изд. - М. : Юстицинформ, 2010. – 200.;
- Рарога, А. И. Уголовное право. Особенная часть: учеб. / под ред. А.И. Рарога. - М., 2011. – 158.
4. Попов, К.И. Компьютерные преступления — преступления мирового масштаба // Правопорядок: история, теория, практика. - 2013. №1 (1) – С. 28 – 31.
5. Российская криминологическая энциклопедия. М.: НОРМА, - 2000. – 258 с.
6. Российская криминологическая энциклопедия. М.: НОРМА, - 2000. – 590 - 591 с.
7. Статистика МВД: данные о совершенных преступлениях по годам: [Электронный ресурс]. – URL: <http://vawilon.ru/statistika-mvd/> (дата обращения: 15.05.2018).