УГОЛОВНЫЙ ПРОЦЕСС, КРИМИНАЛИСТИКА И СУДЕБНАЯ ЭКСПЕРТИЗА

УДК 343.79:681.3

Д.С. АЛПАТОВ,
соискатель

Набережночелнинский филиал Института экономики, управления и права (г. Казань)

ИСПОЛЬЗОВАНИЕ ВЫСОКИХ ТЕХНОЛОГИЙ ПРИ СОВЕРШЕНИИ ОТДЕЛЬНЫХ КАТЕГОРИЙ ПРЕСТУПЛЕНИЙ

В статье рассматриваются возможности использования ЭВМ и всемирной сети Интернет не только в общественно-полезной деятельности, но и при совершении ряда преступных посягательств, таких как хищения чужого имущества, путем мошенничества, посягательств на честь и достоинства личности, некоторых преступлений против общественной безопасности.

Рост высоких технологий, который мы наблюдаем сегодня, в значительной мере влияет на уровень и качество жизни всего человечества, отвечает его интересам и потребностям; процесс развития технологий не только необратим, но и постоянно форсируется. Словосочетание "высокие технологии" (от англ. "high-tech") вряд ли можно считать термином, хотя он является привычным для очень широкого круга людей. Высокие технологии используются как для создания новых продуктов, которые до недавнего времени не были известны и не использовались человечеством, – ракеты, спутники, компьютеры, лазерные устройства, некоторые виды химических соединений, пластиковые и композитные материалы и т.д., так и для улучшения качества и удешевления производства традиционных продуктов. Например, речь может идти о микропроцессорах, встроенных в бытовую технику, – утюги, стиральные машины. Часто, однако, граница является очень зыбкой. Трудно отрицать, что современные автомобили и самолеты – высокотехнологичные продукты, хотя они известны целый век, но также трудно отрицать, что по сравнению со своими предшественниками они приобрели множество новых полезных качеств и функций.

Можно сказать, что в основном развитие высоких технологий, которые могут влиять на будущее, связано с четырьмя направлениями: информационно-коммуникационные технологии, биотехнологии, новые материалы, энергетика.

Стремительное развитие и использование средств телекоммуникаций и компьютерных технологий как одного из основных направлений развития высоких технологий является неотъемлемой частью современного мира. Активное внедрение информационных технологий во все сферы жизни общества породило такое явление, как "компьютерная преступность". Этот термин появился несколько лет назад, когда были выявлены первые случаи преступле-

ний, совершенных с использованием средств телекоммуникаций в ЭВМ.

Кроме того, информатизация современного общества привела к формированию новых видов преступлений, при совершении которых используются вычислительные системы, новейшие средства телекоммуникации и связи, средства негласного получения информации и т.п. За последние 10-15 лет резко увеличилось количество преступлений с использованием вычислительной техники или иной электронной аппаратуры, хищения наличных и безналичных денежных средств. Для совершения преступлений все чаще используются устройства, в основе которых лежат высокоточные технологии их изготовления и функционирования, иными словами, это преступления, в которых используются высокие технологии.

Итак, рассмотрим, каким же образом применяются высокие технологии, в частности компьютеры, электронная аппаратура и средства телекоммуникаций, при совершении преступлений.

Как показывает практика, чаще всего с использованием подобных электронных средств происходят посягательства на собственность, регламентированные главой 21 Уголовного Кодекса России.

Большинство авторов, исследующих этот вопрос, говорят о двух подходах. Наиболее предпочтительным способом, на их взгляд, является оценка ряда преступлений данной главы как совокупности преступлений. Так, с учетом того факта, что Закон "Об информации" определяет понятие собственника информации, а объективной стороной хищения является посягательство на отношения собственности, можно рассматривать незаконное копирование информации как один из видов кражи, и квалифицировать это преступление по совокупности ст. ст. 158 и 272 УК РФ. То есть информация здесь является собственностью юридического или физического лица, на создание и накопление которой были затрачены определенные финансовые и иные ресурсы, например, база данных продаваемых квартир, автомобилей и т.д. Еще одним из подходов является дополнение данной главы новой статьей, предусматривающей ответственность за хищение, где применение компьютерных технологий выступает в качестве способа совершения. Также необходимо отметить, что при совершении определенных категорий преступлений против собственности используются также и иные электронные средства, например, при кражах автомобилей – устройства для удаленного съема сигнала автомобильной сигнализации.

При рассмотрении статьи "Мошенничество" (ст. 159 УК РФ) надо отметить, что большинство преступлений оцениваются по совокупности, например, перепрограммирование игральных автоматов, мошенничество в онлайновой торговле и т.п. – ст. ст. 159 и 272 УК РФ. Типично "хакерское" преступление – "кардинг" – получение информации о владельце кредитной карты, которая позволяет совершать финансовые операции, выдавая себя за владельца кредитной карты. Данное преступление охватывается диспозициями ст. ст. 159 и 272 УК РФ. Далее, в зависимости от поведения преступника ему можно инкриминировать, например, причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ), легализацию (отмывание) денежных средств (ст. 174 УК РФ), изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов (ст. ст. 183, 187 УК РФ). Следует отметить, что данные карты также подделываются с помощью самодельных электронных средств. С помощью высоких технологий совершаются и такие разновидности мошенничества, как, например, в сфере азартных игр (казино, лотереи, тотализаторы), организация финансовых пирамид, фиктивных брачных контор и фирм по оказанию несуществующих услуг [1].

Путем фальсификации компьютерной информации (например подлоги в бухгалтерских и иных учетных документах, "двойная" компьютерная бухгалтерия и т.д.) совершаются преступления, предусмотренные главой 22 УК РФ – Преступления в сфере экономической деятельности, в частности "Незаконное предпринимательство" (ст. 171 УК), "Незаконная банковская деятельность" (ст. 172 УК), "Лжепредпринимательство" (ст. 173 УК) и "Легализация денежных средств, приобретенных преступным путем"

(ст. 174 УК). К тому же здесь применяется по совокупности и ст. 272 УК РФ.

Кроме того, с использованием цветного печатного оборудования и компьютерной обработки изображения преступниками совершается еще одно противоправное деяние – изготовление или сбыт поддельных денег или ценных бумаг (ст. 186 УК РФ).

Компьютерные технологии и средства коммуникаций применяются в таком преступлении, как нарушение авторских и смежных прав (ст. 146 УК РФ). Особенно это наглядно в нашей стране, которая занимает восьмое место в первой десятке стран, где программное обеспечение является контрафактным. Так называемое "компьютерное пиратство" может принимать различные формы, однако можно выделить следующие наиболее распространенные его разновидности – незаконное копирование конечными пользователями, незаконная установка программ на жесткие диски компьютеров, изготовление подделок, установка нелицензионных версий ПО по заказу пользователя, несанкционированный выпуск технической документации. Кроме того, необходимо подчеркнуть ту большую роль, которую играет сегодня Интернет для незаконного копирования и распространения поддельного и иного незаконно распространяемого программного обеспечения. С тех пор как появился Интернет, пиратство приняло особенно большие масштабы. В понятие Интернет-пиратства входит, в частности, использование глобальной сети для рекламы и публикации предложений о продаже, приобретении или распространении пиратских копий программных продуктов. Надо отметить, что нелегальное распространение программного обеспечения по электронной почте, через Интернет и иные информационные сети общего доступа – серьезный вид правонарушений, так как за считанные часы с одного сервера могут быть распространены тысячи копий программного продукта. По аналогии со ст. 146 УК РФ, к ней можно отнести и нарушение изобретательских и патентных прав (ст. 147 УК РФ).

Какие же еще преступления совершаются с помощью средств высоких технологий?

Это преступления против чести и достоинства, предусмотренные в главе 17 УК РФ, а именно статьи "Клевета" (ст. 129 УК) и "Оскорбление" (ст. 130 УК). Клевета – распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию. Оскорбление – унижение чести и достоинства другого лица, выраженное в неприличной форме. Можно отметить, что всемирная сеть Интернет весьма удобна для совершения подобного рода преступлений, например, в целях дискредитации конкурента в бизнесе или в избирательной компании и т.д. [2].

Высокие технологии иногда используются при совершении некоторых преступлений против конституционных прав и свобод человека и гражданина (гл. 19 УК РФ). Например, незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации (ст. 137 УК РФ). Учитывая, что ныне информация о гражданах хранится в огромном количестве автоматизированных баз данных – больниц, банковских учреждений, правоохранительных органов, то, соответственно располагая электронным оборудованием и специальными познаниями, можно ее получить. К таковым также можно отнести и нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных переговоров (ст. 138 УК). В частях 2 и 3 ст. 138 УК указывается на использование технических средств, а также производство, сбыт или приобретение специальных технических средств для негласного получения информации. Кроме того, с использованием высоких технологий может иметь место разглашение тайны усыновления (удочерения), предусмотренные ст. 155 УК РФ.

Применительно к преступлениям против общественной безопасности, предусмотренных главой 24 УК РФ, назовем также состав терроризма (ст. 205 УК) и заведомо ложного сообщения об акте терроризма (ст. 207 УК). Соверше-

ние названных выше преступлений возможно с применением компьютерной сети Интернет. Кроме того, в террористических акциях виновными используются такие средства коммуникации, как радио-, мобильная и пейджинговая связь [3].

В сети Интернет на некоторых сайтах можно найти советы, чертежи, рекомендации по изготовлению огнестрельного оружия и боеприпасов, а также наркотических средств и психотропных веществ, что можно расценивать как интеллектуальное пособничество и квалифицировать по ч. 5 ст. 33 и ст. ст. 223 и 228 УК РФ.

И, наконец, с использованием компьютерных технологий и всемирной сети наиболее часто совершается незаконное распространение порнографических материалов и предметов (ст. 242 УК РФ).

Это далеко не полный перечень преступлений, совершаемых с использованием высоких технологий. Названные выше составы преступлений нуждаются в изменениях и дополнениях, так как действующее уголовное законодательство уже не охватывает всего объема компьютерных правоотношений, и в компьютерной сфере появляются все новые общественно опасные деяния. Развитие законодательства с учетом роста высоких технологий должно привнести точность и ясность в неоднозначно понимаемые в следственно-судебной практике и доктрине вопросы компьютерного права в России.

Список литературы

1. URL: http://www.omamvd.ru
2. URL: http://demo.csm.ru
3. URL: http://www.crime.ru

В редакцию материал поступил 20.03.09.

Ключевые слова: высокие технологии, средства телекоммуникаций и компьютерных технологий, информатизация общества, информация, мошенничество, преступления в сфере экономической деятельности, клевета, нарушение тайны переписки, разглашение тайны.