объединение для совершения преступления против собственности нескольких лиц способствует причинению более существенного материального ущерба; оно повышает степень общественной опасности преступления против собственности. Соучастие в преступлении против собственности наказуемо во всех случаях, а прикосновенная деятельность как менее опасная форма преступного проявления наказуема в случаях, специально указанных в Особенной части УК РФ;

5) основанием для привлечения прикосновенных к преступлениям против собственности лиц к уголовной ответственности выступают совершенные, совершающиеся либо готовящиеся отдельные (некоторые) умышленные преступления против собственности.

На наш взгляд, указанная характеристика признаков прикосновенности к преступлениям против собственности позволяет раскрыть ее содержание и в полной мере отразить особенности объективной и субъективной стороны.

[1] Макаров А.Д. Уголовная ответственность за прикосновенность к преступлению : дис. … канд. юрид. наук. М., 2004. С. 88-89.

[2] Пономаренко Е.В. Некоторые теоретические и законодательные проблемы прикосновенности к преступлению по уголовному праву Российской Федерации : дис. … канд. юрид. наук. Саратов. 2007. С. 69-70.

Бархатова Е.Н.,

кандидат юридических наук

Восточно-Сибирский институт
МВД России (г. Иркутск)

Об общественной опасности мошенничества в сфере высоких технологий

Высокая степень общественной опасности преступлений, совершаемых в сфере высоких технологий, прежде всего с использованием возможностей информационно-телекоммуникационной сети Интернет, вытекает из транснационального характера таких преступлений. Глобальная сеть позволяет людям со всего мира беспрепятственно контактировать. С каждым днем число пользователей продолжает расти, в результате чего создаются условия и для роста числа киберпреступлений.

В настоящее время в мире действуют положения Конвенции о преступности в сфере компьютерной информации от 23 ноября 2001 года. Конвенция предусматривает необходимость обеспечения каждым государством законодательных и иных мер, необходимых для привлечения к уголовной ответственности лиц, осуществляющих неправомерный доступ к компьютерным системам внутри государства в случаях, когда такой доступ является преднамеренным.

Все государства-участники Конвенции тесно сотрудничают друг с другом, применяя соответствующие международные документы о международном сотрудничестве по уголовным делам, связанным с компьютерными системами и данными или со сбором доказательств по уголовному преступлению в электронной форме. Результатом работы в рамках данной Конвенции является оперативное реагирование на несанкционированное вмешательство в информационные системы государств, выявление лиц, совершающих подобные преступления. Российской Федерацией на сегодняшний день данная Конвенция не ратифицирована.

Общественная опасность преступлений, совершаемых в сети Интернет, обусловлена также тем, что преступник, в отличие от других способов совершения преступных деяний, не контактирует с жертвой напрямую, что позволяет ему работать в условиях анонимности. Кроме того, все чаще преступления данного вида совершаются организованными группами.

Среди основных причин киберпреступности в России следует назвать пробелы в законодательстве, регулирующем ответственность за подобные преступления, и разночтения в толковании закона.

Среди самых прибыльных операций, совершаемых хакерами, можно отметить рассылку спама, кражу конфиденциальной информации и Ddos атаки, блокирующие работу сайта.

В сети все более популярными становятся сайты, предлагающие услуги хакеров, что пользуется спросом у преступников. Личные страницы в социальных сетях часто позволяют получать сторонним пользователям значимую информацию о каждом из нас. В связи с этим особое значение приобретает международное сотрудничество, направленное на борьбу с преступлениями в сети Интернет.

Одной из причин, обусловливающих общественную опасность мошенничества в сфере высоких технологий в общем и в сфере компьютерной информации в частности, является недобросовестность работников сферы обслуживания, нарушающих требования информационной безопасности и злоупотребляющих своим служебным положением. Показателен в этом отношении приговор по делу Т.

Т., находясь в должности управляющего офиса обслуживания и продаж, получила доступ к данным клиентов и персональным данным лицевых счетов. Используя доверительные отношения в коллективе, Т. завладела сведениями о конфиденциальных и персональных логинах и паролях других подчиненных ей сотрудников офиса. Обладая доступом к информации о ранее заблокированных сим-картах, Т. под логином и паролем подчиненных ей сотрудников офиса обслуживания и продаж в отсутствие последних на рабочем месте беспрепятственно осуществляла корректировки счетов различных абонентов путем их пополнения за счет средств <…>, а впоследствии переводила денежные средства путем мобильной коммерции на принадлежащие ей банковские карты, абонентские номера знакомых и родственников, а также на банковские счета в счет погашения имеющихся у нее кредитов и путем переводов на имя Л. в счет оплаты услуг за лечение ее малолетнего сына.[1]

Следующим фактором, обусловливающим общественную опасность мошенничества в сфере высоких технологий, является общедоступность последних, что отрицательным образом сказывается на выработке мер предупреждения правонарушений в рассматриваемой сфере.

Также к наиболее общим причинам широкого распространения рассматриваемого вида мошенничества можно отнести слабую осведомленность потерпевших о характере совершаемых ими действий. Так, при «фишинге» мошенник заставляет потерпевшего предоставить конфиденциальную информацию: пароли, информацию о кредитных картах и т.п. Потерпевший, часто не понимая суть совершаемых им же самим действий, выполняет их абсолютно добровольно.

Способы совершения мошенничества в сфере высоких технологий в большинстве случаев характеризуются сложностью и многоэтапностью, что не позволяет органам правопорядка выработать действенные меры по предупреждению и пресечению указанных преступлений.

Мошенничество в сфере высоких технологий в ряде случаев совершается с помощью внедрения соответствующего программного обеспечения, о вредоносности которого потерпевший не подозревает, при этом такое программное обеспечение позволяет нарушать системы защиты цифровой информации, оно находится в свободном доступе в сети Интернет или нелегально приобретается мошенниками на соответствующих виртуальных площадках у его разработчиков.

Как верно отмечает Т.М. Лопатина: «Российская информационная среда отличается несовершенством правовых отношений. В силу этого пользователи, с одной стороны, не могут не балансировать «на грани фола», поскольку далеко не всегда имеются четкие юридические ориентиры правомерного поведения участников информационного процесса. Такое положение обусловливает высокую степень криминологической уязвимости информационной сферы для недобросовестных участников информационных отношений»[2].

Общественная опасность такого рода деяний подтверждается тем фактом, что борьба с преступлениями в сфере компьютерной информации вошла в число приоритетных направлений деятельности правоохранительных органов наряду с противодействием терроризму и коррупции.

В настоящее время все больше применяется межбанковская система электронных платежей, которая не может быть абсолютно надежной. Этим пользуются преступные элементы, которые получают несанкционированный доступ к банковским компьютерным сетям для совершения противоправных действий. Можно сказать, что процесс компьютеризации общества приводит к увеличению количества компьютерных преступлений.

Кроме того, как верно отмечает А.А. Несмеянов, сегодня не существует ни релевантной статистики, позволяющей проанализировать данные, отражающие реальную картину состояния киберпреступности, ни надежных методов сбора таких данных, поэтому нельзя сказать, до какой степени достоверна статистика об экономических потерях в результате совершения преступлений такого рода.[3]

Изложенные факты указывают на достаточно высокую степень общественной опасности мошенничества в сфере высоких технологий и в некоторой степени определяют основные направления противодействия указанному виду преступлений.

---

[1] Приговор Конаковского городского суда Тверской области от 24.07.2014 № 1-171/2014 по делу Т. URL:http://sudact.ru/regular/doc/HkFGuaetNTUP/ (дата обращения: 21.03.2017).

[2] Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности : автореф. дис. … докт. юрид. наук. М., 2006. С. 2.

[3] Несмеянов А.А. Основные проблемы борьбы с преступлениями в сфере высоких технологий / Вестник Восточно-Сибирского института МВД России. 2014. № 4 (71). С. 43-48.

Фисенко Д.Ю.,

кандидат юридических наук

Омская академия МВД России

ОТГРАНИЧЕНИЕ ХИЩЕНИЯ ЧУЖОГО ИМУЩЕСТВА ОТ ПРИСВОЕНИЯ НАЙДЕННОГО ИМУЩЕСТВА

Проблема отграничения хищения чужого имущества от присвоения найденного имущества известна отечественной уголовно-правовой науке и правоприменительной практике уже достаточно давно. Так, ни для кого не секрет, что еще в УК РСФСР 1960 г. наряду с уголовной ответственностью за хищение чужого имущества существовала специальная норма – ст. 148.4 УК РСФСР, предусматривающая уголовную ответственность за присвоение найденного или случайно оказавшегося у виновного чужого имущества, заведомо принадлежащего другому собственнику. В 1996 г., в связи с принятием УК РФ, данное деяние было декриминализовано. Ныне действующее законодательство предусматривает уголовную ответственность только за хищение чужого имущества, в то время как присвоение найденного имущества регламентируется нормами гражданского законодательства (ст. 225-229 ГК РФ) и в определенных законом случаях может повлечь лишь гражданско-правовую ответственность. Однако вплоть до сегодняшних дней «привычка» считать преступлением присвоение найденного имущества глубоко укоренилась в сознании правоприменителя, в связи с чем, несмотря на наличие значительного числа разъяснений и комментариев уголовного закона, в вопросе разграничения хищения и присвоения найденного имущества до сих пор не поставлена точка.

Кроме того, с недавних пор данная проблема усугубилась в связи с кассационным определением Верховного Суда