

МОДИФИКАЦИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК СПОСОБ ПРИЧИНЕНИЯ ИМУЩЕСТВЕННОГО УЩЕРБА БЕЗ ПРИЗНАКОВ ХИЩЕНИЯ*

*Д.Г. МОРОЗ, преподаватель кафедры уголовного права
Белорусского государственного университета ©*

Важнейшими признаками причинения имущественного ущерба при отсутствии признаков хищения являются способы осуществления данного преступления. Модификация компьютерной информации является новым способом совершения преступления, ответственность за реализацию которого предусмотрена статьей 216 Уголовного кодекса (УК) Республики Беларусь. Данный способ причинения имущественного ущерба без признаков хищения был впервые предусмотрен статьей 250 Модельного УК для государств-участников СНГ. В уголовном праве модификация компьютерной информации может иметь различное значение. В одном случае модификация компьютерной информации может выступать в качестве самостоятельного уголовно наказуемого деяния (ст. 350 УК). В других случаях модификация компьютерной информации выступает уже в качестве способа совершения некоторых преступлений против собственности (ст. 212 и 216 УК). Дается уголовно-правовая характеристика модификации компьютерной информации как способа причинения имущественного ущерба при отсутствии признаков хищения.

Первые исследования, посвященные проблеме компьютерных преступлений на территории бывшего СССР, были осуществлены в конце 1980-х – начале 1990-х годов. Существенным вкладом в развитие доктрины уголовного права в сфере компьютерных преступлений явилась вышедшая в 1991 году монография Ю.М. Батурина и А.М. Жодзинского «Компьютерные преступления и компьютерная безопасность» [1]. Авторы предложили классифицировать компьютерные преступления на два вида: а) посягательства, при совершении которых компьютеры используются как техническое средство совершения иного преступления; б) преступления, связанные с вмешательством в работу компьютера. В первом случае компьютер используется как орудие совершения иного преступления, а во втором – речь идет о преступном вмешательстве в сферу обращения с компьютерной информацией. Представляется, что причинение имущественного ущерба без признаков хищения путем модификации компьютерной информации следует отнести к первой категории преступлений с использованием компьютерных технологий.

Вопросам уголовно-правовой борьбы с компьютерными преступлениями посвящены работы таких российских ученых, как В.А. Мазуров [2], В.Б. Вехов [3], В.В. Крылов [4].

Среди отечественных ученых-криминалистов исследованию уголовно-правовых аспектов

безопасности в сфере компьютерных технологий посвятили свои работы Н.Ф. Ахраменка [5], В.Е. Козлов [6], А. Лепехин [7], В. Лосев [8].

Некоторыми учеными высказывается точка зрения, в соответствии с которой предлагается исключить модификацию компьютерной информации из числа способов совершения преступления, предусмотренного статьей 216 УК. Так, аргументы белорусского исследователя А. Лепехина сводятся к тому, что сложно разграничить модификацию компьютерной информации как самостоятельного уголовно наказуемого деяния, предусмотренного статьей 350 УК, и причинение имущественного ущерба без признаков хищения путем модификации компьютерной информации [7, с.58]. При этом необоснованно и механически признаки модификации компьютерной информации как самостоятельного уголовно наказуемого деяния переносятся на модификацию компьютерной информации как способа совершения иного преступления – причинения имущественного ущерба без признаков хищения.

В толковом словаре по информатике модификация определяется как любые изменения, не меняющие сущности объекта. При этом модификация базы данных (в т.ч. информационной) может осуществляться посредством реструктурирования, реорганизации, а также обновления содержания ее файлов, добавления, удаления записей [9; с. 209]. В уголовно-правовой литературе модификация компьютерной информации опре-

* Статья поступила в редакцию 6 августа 2007 года.

деляется как видоизменение, характеризующееся появлением новых свойств [10; с.8–15]. Некоторые авторы полагают, что под модификацией компьютерной информации понимается внесение в нее любых изменений, порождающих ее отличие от той, которая была введена в систему и которой владеет собственник информационного ресурса [12; с.104].

По нашему мнению, не всякое изменение компьютерной информации может выступать в качестве способа причинения имущественного ущерба без признаков хищения. В определенных случаях модификация компьютерной информации может преследовать общественно полезные цели. Следовательно, модификация компьютерной информации может выступать в качестве способа рассматриваемого состава преступления только в том случае, если вносимые изменения носят *противоправный* характер.

Противоправность модификации компьютерной информации при совершении преступления, предусмотренного статьей 216 УК, может находить свое выражение в следующих возможных формах преступного поведения: а) либо лицо, модифицирующее компьютерную информацию, осуществляет эту операцию на законном основании, однако вносимые изменения по своему содержанию направлены на достижение преступного результата; б) либо лицо, модифицирующее информацию, вообще не имеет законных оснований на осуществление этой операции. Таким образом, сама модификация компьютерной информации может осуществляться как на законном, так и на незаконном основании. Для установления признаков состава преступления, предусмотренного статьей 216 УК, важно установить направленность модификации компьютерной информации на причинение имущественного ущерба без признаков хищения, что и определяет противоправность анализируемого способа совершения преступления.

Модификация компьютерной информации при отсутствии законных оснований на реализацию этой операции осуществляется в результате *несанкционированного доступа к компьютерной информации*. По нашему мнению, модификация компьютерной информации, сопряженная с несанкционированным доступом к ней, должна выступать в качестве *квалифицированного* признака причинения имущественного ущерба без признаков хищения. Несанкционированный доступ к компьютерной информации значительно увеличивает *степень общественной опасности* причинения имущественного ущерба без признаков хищения путем модификации компьютерной информации. Это определяется следующим: модификация компьютерной информации, осуществляемая посредством несанкционированного доступа к ней, при совершении преступления, предусмотренного статьей 216 УК, причиняет вред не только имущественным отношениям, но и

информационной безопасности. Несанкционированный доступ к компьютерной информации сопряжен с нарушением системы защиты компьютерной системы, что может повлечь блокирование, уничтожение или приведение в непригодное состояние компьютерной информации. Помимо этого, несанкционированный доступ к компьютерной информации даже в том случае, если виновный стремится совершить только деяние, предусмотренное статьей 216 УК, содержит в себе угрозу раскрытия государственной, военной, коммерческой и иной охраняемой законом тайны [2, с.36–38].

Наряду с этим следует отметить, что несанкционированный доступ к компьютерной информации выступает в качестве квалифицированного признака хищения путем использования компьютерной техники (ч. 2 ст. 212 УК), а также преступления, ответственность за совершение которого предусмотрена части 2 статьи 350 УК. Представляется, что в целях обеспечения единообразного подхода к установлению уголовной ответственности за преступления, совершаемые посредством модификации компьютерной информации, сопряженной с несанкционированным доступом к ней, целесообразно данное обстоятельство (несанкционированный доступ) установить в качестве квалифицированного признака не только в части 2 статьи 212 и части 2 статьи 350 УК, но также и в части 2 статьи 216 УК.

При определенных обстоятельствах компьютерная информация может быть использована при совершении участниками гражданского оборота действий имущественного характера. В свою очередь она должна обладать определенными реквизитами, позволяющими идентифицировать ее как электронный документ.

В соответствии со статьей 6 Закона Республики Беларусь от 10 января 2000 года «Об электронном документе» электронный документ должен соответствовать следующим требованиям:

- создаваться, обрабатываться, передаваться и храниться с помощью программных и технических средств;
- иметь структуру, установленную данным Законом, и содержать реквизиты, позволяющие его идентифицировать;
- быть представленным в форме, понятной для восприятия человеком.

В случае причинения имущественного ущерба без признаков хищения путем модификации компьютерной информации преступник совершает действия, направленные на изменение непосредственно самого содержания электронного документа. В результате преступник получает возможность, к примеру, уклониться от передачи вознаграждения лицу, чьим имуществом или чьими услугами (связь, коммунальное обслуживание, кабельное телевидение и др.) он воспользовался.

В том случае, если преступник посредством модификации компьютерной информации вносит

в электронный документ сведения, указывающие в качестве приобретателя имущества или пользователя услуг третье лицо, то в данном случае имущественный ущерб без признаков хищения причиняется иному лицу, а не собственнику (законному владельцу) имущества, либо лицу, оказывающему услуги. В данной ситуации виновный вынуждает расплатиться вместо себя третье лицо, которому в свою очередь и причиняется имущественный ущерб без признаков хищения в виде **реального имущественного ущерба**.

Исходя из вышесказанного, следует признать ошибочной квалификацию судом Октябрьского района г. Минска деяния, совершенного М., который *по предварительному сговору с другим лицом вводил в компьютерную систему другую информацию. Это выразалось в предоставлении в интернет-магазина с использованием международной сети Интернет номеров, не принадлежащих им кредитных карт и заведомо недостоверных сведений об их владельцах. Выступая от их имени для оплаты товара, заказываемого по электронной почте для себя на имена третьих лиц, проживающих в г. Минске, М. безвозмездно завладел имуществом предприятий иностранных государств в особо крупном размере на общую сумму 23 960 долларов США. Действия М. квалифицированы по части 4 статьи 212 УК как хищение имущества путем введения в компьютерную систему ложной информации, совершенного группой лиц по предварительному сговору в особо крупном размере* [10, с.54].

По нашему мнению, суд, квалифицируя данное деяние, не учел, что М. *оплачивал* свои покупки в зарубежных интернет-магазинах за счет кредитных карт, принадлежащих другим лицам. Таким образом, М. не причинял иностранным интернет-магазинам имущественного ущерба посредством хищения принадлежащего им имущества, поскольку в данном случае отсутствует один из существенных признаков хищения – **безвозмездность** завладения чужим имуществом или правом на него. Имущественный ущерб в этой ситуации причинен владельцам кредитных карт. Причинение виновным имущественного вреда в данном случае характеризуется отсутствием признаков хищения, поскольку виновный, непосредственно **не завладевая** принадлежащими владельцам кредитных карт денежными средствами, путем компьютерных манипуляций производил расчет за приобретаемый в интернет-магазинах товар.

Воздействие на компьютерную информацию может осуществляться посредством ее **злонамеренной вирусной модификации**. Под этим понимается разработка, использование либо распространение программ-вирусов, которые заведомо приводят к нарушению работы ЭВМ или их сетей, внесение несанкционированных изменений

в компьютерную информацию [6, с.27–28]. Отметим, что само по себе использование вредоносных программ с целью несанкционированного уничтожения, блокирования, модификации информации, хранящейся в компьютерной системе, сети или на машинных носителях влечет ответственность в соответствии со статьей 354 УК. Вследствие этого причинение имущественного ущерба без признаков хищения посредством злонамеренной вирусной модификации компьютерной информации следует квалифицировать по совокупности преступлений, ответственность за совершение которых предусмотрена статьями 216 и 354 УК.

Для более точного установления признаков модификации компьютерной информации как способа совершения преступления необходимо отграничивать данный состав преступления от составов преступлений, в качестве одного из конструктивных признаков которых также выступает модификация компьютерной информации. К таковым относятся: хищение путем использования компьютерной техники (ст. 212 УК) и модификация компьютерной информации (ст. 350 УК).

При совершении преступлений, предусмотренных статьями 212 и 216 УК, модификация компьютерной информации выступает в качестве одного и того же признака объективной стороны состава преступления, а именно способа совершения преступления. Причем при хищении путем использования компьютерной техники и при причинении имущественного ущерба без признаков хищения преступник использует модификацию компьютерной информации как способ посяательства на имущественные интересы потерпевшего. Тем не менее, при совершении преступления, предусмотренного статьей 212 УК, модификация компьютерной информации выступает в качестве способа противоправного безвозмездного завладения чужого имущества или права на него. При совершении преступления, предусмотренного статьей 216 УК, виновный не завладевает чужим имуществом или правом на него, а путем модификации компьютерной информации: а) либо противоправно пользуется чужим имуществом; б) либо уклоняется от передачи должного; в) либо обманным путем вынуждает потерпевшего расплатиться вместо себя за оказанные услуги или пользование чужим имуществом; г) либо обращает в свою пользу или пользу третьих лиц имущество, которое должно было поступить потерпевшему.

Особенностями отграничения причинения имущественного ущерба без признаков хищения путем модификации компьютерной информации от модификации компьютерной информации как самостоятельного преступления являются то, что:

1) основным объектом причинения имущественного ущерба без признаков хищения путем модификации компьютерной информации выступают

отношения собственности. Основным объектом модификации компьютерной информации как самостоятельного преступного деяния выступает **информационная безопасность;**

2) при совершении преступления, предусмотренного статьей 350 УК, модификация компьютерной информации является самостоятельным уголовно наказуемым **деянием.** При совершении преступления, предусмотренного статьей 216 УК, модификация компьютерной информации выступает в качестве **способа** осуществления иного уголовно наказуемого деяния – причинения имущественного ущерба без признаков хищения;

3) причинение имущественного ущерба без признаков хищения путем модификации компьютерной информации может быть совершено только с **прямым умыслом.** В тоже время модификация компьютерной информации как самостоятельное уголовно наказуемое деяние может быть совершено **как с прямым, так и с косвенным умыслом;**

4) при совершении преступления, предусмотренного статьей 216 УК, модификация компьютерной информации направлена на достижение **корыстной** цели – извлечение выгоды имущественного характера вследствие причинения имущественного ущерба без признаков хищения. При совершении преступления, предусмотренного статьей 350 УК, виновный такой цели не преследует.

Таким образом, признаками модификации компьютерной информации как способа причинения имущественного ущерба без признаков хищения являются:

- внесение изменений в компьютерную информацию является противоправным;
- внесение изменений в компьютерную информацию осуществляется с корыстной целью;
- внесение изменений в компьютерную информацию направлено на причинение имущественного ущерба без признаков хищения;
- внесение с помощью аппаратных и программных средств ЭВМ в компьютерную информацию каких-либо изменений либо внесение в компьютерную систему заведомо ложной информации.

Таким образом, модификацию компьютерной информации как способ причинения имущественного ущерба без признаков хищения можно охарактеризовать как **противоправное, с корыстной целью, внесение посредством аппаратных или программных средств ЭВМ в компьютерную информацию каких-либо изменений, либо введение в компьютерную систему заведомо ложной информации.**

В целях обеспечения единообразного подхода к установлению уголовной ответственности за преступления, совершаемые посредством модификации компьютерной информации, сопряженной с несанкционированным доступом к ней, целесообразно данное обстоятельство установить в качестве квалифицированного признака в части 2 статьи 216 УК, посягательства против собственности, осуществляемые путем модификации компьютерной информации и не сопряженные с безвозмездным завладением чужого имущества должны квалифицироваться в соответствии со статьей 216 УК.

ЛИТЕРАТУРА

1. Батурин, Ю.М. Компьютерные преступления и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзинский. – М., 1991.
2. Мазуров, В.А. Компьютерные преступления: классификация и способы противодействия / В.А. Мазуров. – М., 2002.
3. Вехов, В. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ / В. Вехов // Уголовное право. – 2004. – №4.
4. Крылов, В. Криминалистические проблемы оценки преступления в сфере компьютерной информации / В. Крылов // Уголовное право. 1998. №3. С. 81–89; Крылов В.В. Расследование преступлений в сфере информации. М.: Городец, 1998; Крылов, В.В. Информационные компьютерные преступления / В.В. Крылов. – М.: НОРМА-ИНФРА М, 1997.
5. Ахраменка, Н.Ф. Глава 31. Преступления против информационной безопасности / Н.Ф. Ахраменка // Комментарий к Уголовному кодексу Республики Беларусь / Н.Ф. Ахраменка, Н.А. Бабий, А.В. Барков [и др.]; под общ. ред. А.В. Баркова, В.М. Хомича. – Минск: ГИУТС БГУ, 2007.
6. Козлов, В.Е. Компьютерные преступления: криминалистическая характеристика и осмотр места происшествия / В.Е. Козлов. – Минск: Академия МВД Республики Беларусь, 2001.
7. Лепехин, А. Преступления против информационной безопасности: правовые аспекты / А. Лепехин // Судовы веснік. – 2006. – №1.
8. Лосев, В. Преступления против информационной безопасности / В. Лосев // Судовы веснік. – 2002. – №1.
9. Першиков, В.И. Толковый словарь по информатике / В.И. Першиков, В.М. Савинков. – М.: Финансы и статистика, 1995.
10. О судебной практике по делам о хищении имущества (по материалам обзора судебной практики) // Судовы веснік. – 2002. – №1.