УДК 343.985

Е. А. Леоненя
Учреждение образования «Барановичский государственный университет», Барановичи

ХИЩЕНИЕ ПУТЕМ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ТЕХНИКИ КАК ОПАСНОЕ ПРЕСТУПЛЕНИЕ ПРОТИВ СОБСТВЕННОСТИ

Введение. Актуальность вопросов, связанных с уголовной ответственностью за хищения, совершаемые с использованием информационных технологий, обусловлена тем, что в настоящее время правонарушения, посягающие на отношения собственности и непосредственно связанные с использованием компьютерных технологий и сети Интернет, получили широкое распространение и приобрели ярко выраженный интернациональный характер. В абсолютном большинстве случаев лица не знают друг друга в реальной жизни, их взаимодействие реализуется посредством виртуальных средств идентификации [1].

Соответственно, обеспечение безопасности в информационной сфере требует постоянного поиска новых механизмов противодействия киберпреступности, включая правовые инструменты, анализа причин, рисков и угроз высокотехнологичных преступлений против собственности. Кроме того, интернационализация киберпреступлений делает необходимой активизацию процесса унификации и развития уголовного законодательства Республики Беларусь. В связи с этим происходит глубокое реформирование ключевых отраслей действующего законодательства, в ходе которого существенно изменяются и дополняются уже существовавшие нормы [2, с. 199].

Основная часть. В настоящее время общее определение хищения закреплено в п. 1 примечаний к главе 24 Уголовного кодекса Республики Беларусь (далее — УК) в качестве умышленного противоправного безвозмездного завладения чужим имуществом или правом на имущество с корыстной целью путем кражи, грабежа, разбоя, вымогательства, мошенничества, злоупотребления служебными полномочиями, присвоения, растраты или использования компьютерной техники [3].

Как отмечает И. О. Грунтов, объективная сторона хищения, предусмотренного ст. 212 УК, отличается способом нарушения отношений собственности, а именно путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации [4]. При этом в п. 20 постановления Пленума Верховного Суда Республики Беларусь от 21 декабря 2001 года № 15 «О применении судами уголовного законодательства по делам о хищениях имущества» (Постановление № 15) внимание судов обращается на то, что данное хищение возможно лишь посредством компьютерных манипуляций, заключающихся в обмане потерпевшего или лица, которому имущество вверено или под охраной которого оно находилось, с использованием системы обработки информации [5].

Вместе с тем В. В. Хилюта обращает внимание на то, что обман как способ совершения мошенничества может быть средством, облегчающим совершение преступления с использованием компьютерной техники, однако в таком случае состав, предусмотренный ст. 212 УК, будет отсутствовать. Обусловлено это тем, что суть компьютерных манипуляций не может заключаться в обмане, поскольку лицо, работающее с системами автоматизированной обработки информации, объективно поставлено в такие условия, что оно будет добросовестно заблуждаться относительно полученной информации, независимо от того, была ли она видоизменена или изначально являлась ложной. Другими словами, использование компьютерных манипуляций не ведет к обману, поскольку в данном случае отсутствует как таковой обман живого человека [6].

По этим причинам отсутствует состав преступления, предусмотренный ст. 212 УК в таких широко распространенных схемах мошенничества, как рассылка электронных сообщений через социальные сети и электронную почту либо размещение объявлений на специализированных сайтах в сети Интернет, где компьютер используется лишь как инструмент для установления контакта с потенциальными жертвами. Характерным примером может послужить приводимый В. В. Белокопытовым и В. М. Филиппенковым мошеннический прием знакомства с помощью Интернета через различные социальные сети в целях хищения денежных средств, переводимых несостоявшимися «невестами» на электронный адрес предполагаемого «жениха». Причем в Республике Беларусь установлены факты, когда женщины различного возраста переводили мошенникам десятки тысяч долларов США, продавая в отдельных случаях даже собственную квартиру либо занимая валютные средства в банке. Еще одним примером является так называемое «сетевое попрошайничество», а также деятельность фальшивых сборщиков пожертвований для спасения больных детей, бездомных животных и т. п. Нередкими на практике являются и случаи, когда мошенники предлагают различные товары, причем по цене значительно ниже рыночной, принимают предоплату с банковской карты или электронного кошелька жертвы, после чего исчезают. Схожим образом действуют те злоумышленники, которые предлагают выгодную работу через Интернет, получить которую можно только после оплаты «обучающих курсов» [7].

Поскольку в подобных деяниях не происходит манипуляции с компьютерными данными и компьютерной информацией и хищение имущества не является следствием этих манипуляций, такие действия охватываются традиционными нормами о мошенничестве и не требуют квалификации по специальным нормам ст. 212 УК.

В рамках специальных составов преступлений, предусмотренных ст. 212 УК, исследователями в области уголовного права и криминалистики также предпринимаются попытки классификации данной формы хищений. В частности, С. В. Воронцова выделяет такие способы совершения мошенничества:

– фишинг, при котором пользователей заманивают на фальшивые сайты, где получают доступ к данным платежных карт в целях хищения денежных средств;

– фарминг, когда происходит перенаправление на ложный IP-адрес (например, вместо сайта системы дистанционного обслуживания банка пользователи попадают на мошеннический сайт, где вводят свои персональные данные для проведения платежей);

– кардинг, т. е. производство расчетных операций с использованием не инициированной (или не подтвержденной) ее владельцем банковской карты или ее реквизитов [8].

Поскольку в диспозиции ст. 212 УК компьютерная техника выступает в качестве средства совершения хищения и преступник прибегает к искажению передаваемой информации, актуальным вопросом уголовной ответственности за хищения, совершаемые с использованием информационных технологий, является разграничение данных преступлений от составов преступных деяний, ответственность за которые предусмотрена статьями главы 31 УК «Преступления против информационной безопасности». Н. А. Швед подчеркивает, что, криминализировав несанкционированный доступ к компьютерной информации путем закрепления его в статье, открывающей главу 31 УК, законодатель, по сути, определил фундамент компьютерных преступлений, сформулированных с ориентацией на признаки этого состава преступления [9].

Одновременно законодатель предусмотрел несанкционированный доступ и в качестве квалифицирующего признака иных преступлений: в частности, в ч. 2 ст. 212 УК несанкционированный доступ к компьютерной системе или сети, где хранится информация, т. е., по сути, к компьютерной информации, выступает в качестве квалифицирующего признака хищения имущества путем использования компьютерной техники.

Что касается субъективных признаков, то бесспорным представляется факт совершения преступления, предусмотренного ст. 212 УК, по корыстным мотивам. Такой же признак, как «иная личная заинтересованность», по справедливому замечанию В. В. Хилюты, не может служить основанием для того, чтобы квалифицировать хищение путем использования компьютерной техники, сопряженное с несанкционированным доступом к компьютерной информации, по совокупности ч. 2 ст. 212 и ч. 2 ст. 349 УК, поскольку последствия, о которых говорится в п. 21 Постановления № 15, в ч. 2 ст. 349 УК не предусмотрены. Такие последствия (крушение, авария, катастрофа, несчастные случаи с людьми) теоретически могут наступить лишь в результате неосторожных действий лица (ч. 3 ст. 349 УК), совершающего хищение с помощью компьютерной техники [6].

Заключение. Белорусский законодатель рассматривает хищение с помощью компьютерной техники в качестве самостоятельной формы хищения, о чем свидетельствует наличие отдельной ст. 212 в нормах УК, а также п. 1 примечаний к главе 24 УК. Установление уголовной ответственности за хищения, совершаемые с использованием информационных технологий, в Беларуси обусловлено таким их признаком, как общественная опасность. Данный признак присущ преступлениям, является их ключевой характеристикой, тогда как иные правонарушения подобной степенью вредоносности по отношению к охраняемым уголовным законом общественным отношениям не обладают. Более того, хищения, совершаемые с использованием информационных технологий, относятся к преступлениям против собственности, а их криминализация обусловлена значимостью отношений собственности и ее правовой природой как абсолютного вещного права, гарантированного Конституцией Республики Беларусь. Необходимость установления уголовной ответственности за хищения, совершаемые с использованием информационных технологий, обусловлена спецификой способов и средств совершения данных преступлений против собственности, их совершением группой лиц, в том числе с вовлечением в преступную деятельность несовершеннолетних.

Список цитируемых источников

1. *Дмитренко, А. П.* О нетипичных аспектах соучастия в преступлениях, совершаемых с использованием информационно-коммуникационных технологий / А. П. Дмитренко, Е. А. Русскевич // Вестн. Акад. Генер. прокуратуры Рос. Федерации. — 2017. — № 5 (61). — С. 18—20.
2. *Осокин, Р. Б.* К вопросу об организации деятельности органов прокуратуры в Российской Федерации (основные функции, принципы) / Р. Б. Осокин // Вестн. Моск. ун-та МВД России. — 2015. — № 9. — С. 199—202.
3. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : в ред. Закона Респ. Беларусь от 11.11.2019 г. № 253-З // Нац. правовой Интернет-портал Респ. Беларусь. — 23.11.2019. — 2/2691.
4. Основы квалификации преступлений : учеб. пособие. — 2-е изд., перераб. и доп. — М. : Проспект, 2011. — 61 с.
5. Научно-практический комментарий к Уголовному кодексу Республики Беларусь / Н. Ф. Ахраменка [и др.] ; под ред. А. В. Баркова, В. М. Хомича. — 2-е изд., с изм. и доп. — Минск : ГИУСТ БГУ, 2010. — 1007 с.
6. *Хилюта, В. В.* Хищение: понятие, признаки, проблемы квалификации : монография / В. В. Хилюта. — Гродно : ГрГУ, 2011. — 335 с.
7. *Белокопытов, В. В.* Особенности совершения и предупреждения киберпреступлений / В. В. Белокопытов, В. М. Филиппенко // ИБ «Комментарии законодательства». — Минск : ЮрСпектр, 2020.
8. *Воронцова, С. В.* Киберпреступность: проблемы квалификации преступных деяний / С. В. Воронцова // Рос. юстиция. — 2011. — № 2. — С. 14—15.
9. *Сивицкая, Н. А.* Уголовное законодательство зарубежных стран об ответственности за несанкционированный доступ к компьютерной информации / Н. А. Сивицкая // Проблемы правовой информатизации. — 2007. — № 1. — С. 61—64.