УГОЛОВНОЕ ПРАВО, КРИМИНОЛОГИЯ

УДК 343.534

ОБЪЕКТИВНЫЕ ПРИЗНАКИ НЕПРАВОМЕРНОГО ЗАВЛАДЕНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИЕЙ

М.А. ДУБКО
(Белорусский государственный университет, Минск)

Дается уголовно-правовая характеристика объективных признаков неправомерного завладения компьютерной информацией как преступления против информационной безопасности. В частности, рассматриваются особенности объекта и предмета преступного посягательства, а также элементы объективной стороны рассматриваемого состава. Анализ статистических данных о зарегистрированных в Беларуси преступлениях в сфере высоких технологий показал тенденцию постоянного роста количества преступлений данной категории. Показаны два варианта выхода из сложившейся ситуации.

Введение. Всё возрастающее значение и широкое применение компьютерных технологий в современном обществе несет в себе наряду с бесспорно позитивными проявлениями угрозу противоправного их использования. Компьютерная информация сегодня стала одним из важнейших ресурсов человечества и все чаще становится предметом преступного посягательства. Принятый в 1999 году Уголовный кодекс Республики Беларусь предусматривает уголовную ответственность за неправомерное завладение компьютерной информацией. Точное установление объективных признаков рассматриваемого состава служит предпосылкой верной квалификации совершенного деяния, отграничения от смежных составов и иных правонарушений. Однако часто в правоприменительной практике установление и определение обязательных признаков объективной стороны неправомерного завладения компьютерной информацией, закрепленных в диспозиции статьи 352 Уголовного кодекса Республики Беларусь (далее – УК), вызывает затруднение и может привести к ошибочной квалификации деяния.

Основная часть. Исследование проблем объекта преступления имеет важное теоретико-прикладное значение. Это объясняется тем, что установление объекта – начальный этап квалификации и признание деяния как преступления. Наука уголовного права традиционно выделяет понятие общего, родового, видового и непосредственного объектов преступления.

В главу 31 УК «Преступления против информационной безопасности» законодатель включил семь составов преступлений, предусматривающих уголовную ответственность за общественно опасные деяния, посягающие на единый объект уголовно-правовой охраны, – общественные отношения, обеспечивающие информационную безопасность государственных и частных интересов. Под информационной безопасностью как частью национальной безопасности следует понимать состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [1]. Таким образом, родовым объектом рассматриваемой группы преступлений являются общественные отношения по обеспечению защищенности от внешних и внутренних угроз сферы оборота компьютерной информации, а также нормального функционирования компьютера, компьютерной системы или сети. Непосредственным объектом неправомерного завладения компьютерной информацией являются общественные отношения, устанавливающие порядок получения и распространения информации, хранящейся в компьютерной системе, сети или на машинном носителе, либо информации, передаваемой с использованием средств компьютерной связи.

Особенности предмета преступления тесно связаны с объектом уголовно-правовой охраны и, соответственно, со степенью общественной опасности совершаемого преступления. Предметом преступления (в широком понимании) выступают те социальные блага, по поводу которых возникают и существуют общественные отношения и воздействуя на которые виновный нарушает эти отношения [2, с. 105]. В соответствии с данным определением предметом преступления могут быть любые социальные блага, как материальные, так и нематериальные ценности. Полагаем, что при определении предмета неправомерного завладения компьютерной информацией необходимо придерживаться предлагаемого в научной литературе широкого понятия предмета преступления, включающего, кроме вещей, и различные нематериальные ценности. При неправомерном завладении предметом преступления является информация, хранящаяся в компьютерной системе, сети или на машинных носителях, а также информация, передаваемая с использованием средств компьютерной связи (компьютерная информация), т.е. содержащаяся в устройствах ее передачи – в устройствах связи, сетевых устройствах, представляющих собой среду ее распространения [3, с. 821]. Единственное официальное определение компьютерной информации за-

креплено в Соглашении государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации 2001 года [10, с. 25], однако данное соглашение подписано более 10 лет назад и не в полной мере соответствует реалиям современного общества.

Анализируя научную литературу, все существующие определения компьютерной информации можно разделить на две группы:

1) определения, которые характеризуют компьютерную информацию исходя из формы ее представления. В Белорусской юридической энциклопедии Н.Ф. Ахраменка приводит следующее определение: сведения, которые хранятся, обрабатываются, передаются в компьютерах, компьютерных системах, сетях в дискретной или непрерывной формах [9, с. 70];

2) определения, которые в толковании данного понятия исходят из содержательного аспекта информации. Так, например, в примечании к новой редакции статьи 272 УК Российской Федерации (Неправомерный доступ к компьютерной информации) российским законодателем дается официальное толкование компьютерной информации – сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [4].

При определении компьютерной информации как предмета неправомерного завладения следует учесть два этих подхода и исходить из анализа родового объекта преступлений против информационной безопасности, содержания диспозиции статьи 352 Уголовного кодекса Республики Беларусь, а также руководствоваться терминологией, которую использует законодатель. Таким образом, компьютерную информацию можно определить как сведения (сообщения, данные), хранящиеся на компьютере или обрабатываемые им, доступные для восприятия компьютером либо передающиеся по линиям связи. Под компьютером стоит понимать любое устройство, предназначенное или способное хранить, обрабатывать или передавать информацию.

Объективная сторона является исходным началом для установления других элементов и признаков состава преступления и влияет на определение характера и степени общественной опасности совершенного деяния. Объективная сторона рассматриваемого состава преступления включает деяние, общественно опасные последствия и причинную связь между ними. Общественно опасное деяние как обязательный признак неправомерного завладения компьютерной информацией может выражаться лишь в форме общественно опасного действия – активное поведение субъекта, выражающееся в нарушении установленного порядка получения и распространения компьютерной информации путем определенных телодвижений, направленных на завладение компьютерной информацией, что может и должно вызвать причинение вреда субъекту посягательства. Рассматривая общественно опасное деяние, совершенное в форме действия, следует иметь в виду, что такое деяние может быть признано общественно опасным только в том случае, если оно является осознанным и волевым, т.е. при отсутствии признаков непреодолимой силы, физического или психического принуждения. Неправомерно завладеть компьютерной информацией путем бездействия не представляется возможным.

Таким образом, деяние выражается в активных действиях, которые могут быть совершены одним из альтернативно перечисленных в диспозиции способов: несанкционированное копирование компьютерной информации; перехват компьютерной информации; иное неправомерное завладение компьютерной информацией.

Закон Республики Беларусь от 10 ноября 2007 года «Об информации, информатизации и защите информации» определяет правовой режим информации, а также регулирует общественные отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации. Копирование компьютерной информации с нарушением ее правового режима, установленного нормативными актами или собственником, рассматривается уголовным законом как несанкционированное: лицо либо не имеет право копировать данную информацию, либо обладает таким правом, но нарушает установленный порядок совершения этих действий.

Несанкционированное копирование – повторное и устойчивое запечатление компьютерной информации на машинном или ином носителе без разрешения собственника, владельца, уполномоченных ими лиц или законного пользователя или распечатывание этой информации на средствах компьютерной техники. Не обязательно, чтобы исходная компьютерная информация копировалась в неизменном виде. Полагаем, что уголовно-наказуемым должно считаться несанкционированное копирование, например, части базы данных, выборочных данных из общего массива информации, изготовление копии целого или части путем рукописного ввода информации на цифровой или бумажный носитель при визуальном доступе к компьютерной информации. Запечатление компьютерной информации в памяти человека, например, при визуальном восприятии, с последующим закреплением в любой материальной форме такой информации, на наш взгляд, также можно отнести к копированию. Исходя из сказанного, при определении объективной стороны рассматриваемого состава под несанкционированным копированием следует понимать изготовление копий *содержания* компьютерной информации без разрешения собственника или иного уполномоченного субъекта.

Исходная копируемая информация при этом изменениям и повреждениям не подвергается. Собственник или иной законный владелец не утрачивает возможность использования ее по назначению. Вид

задействованных в копировании первичных и вторичных машинных носителей (магнитный или оптический носитель, бумага) значения не имеет.

В юридической литературе встречается и более широкий подход к понятию копирования, отождествляющий копирование информации с ее распространением и разглашением [5, с. 235 – 236]. Представляется, что использование понятий «распространение», «разглашение» из авторского права для раскрытия содержания используемого в Уголовном законе понятия «копирование» необоснованно, так как объекты статьи 201 УК «Нарушение авторских, смежных, изобретательских и патентных прав» и главы 31 УК Беларуси различны.

Общественная опасность исключительно несанкционированного копирования компьютерной информации, на наш взгляд, обусловлена особенностями предмета рассматриваемого преступления. Однако было бы правильным рассматривать основанием уголовной ответственности за неправомерное завладение компьютерной информацией случаи, когда неправомерное завладение (копирование) сопряжено с причинением существенного вреда, т.е. такому завладению следовало бы придать значение не только причины, но и необходимого условия. Практика показывает, что при неправомерном завладении компьютерной информацией не всегда причиняется существенный вред либо его трудно оценить (измерить), в связи с чем степень общественной опасности совершенного деяния становится значительно меньше. Однако при этом все же нарушаются общественные отношения, устанавливающие порядок получения компьютерной информации. В связи с этим предлагаем включить в главу 22 «Административные правонарушения в области связи и информации» Кодекса Республики Беларусь об административных правонарушениях норму, предусматривающую административную ответственность за неправомерное завладение компьютерной информацией, не повлекшее причинение существенного вреда. Устанавливать уголовную ответственность за повторное совершение данного деяния в течение года после наложения административного взыскания, полагаем, нецелесообразно.

Перехват информации, передаваемой с использованием средств компьютерной связи, – это неправомерное завладение компьютерной информацией в устройствах, которые ее не хранят, а только передают (перемещают) ее в пространстве: незаконное подключение к линиям связи, включение в программы специальных блоков типа «троянский конь», дистанционный съем информации с различных технических устройств за счет их побочных электромагнитных излучений и наводок, принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей частоты [3].

Так, В.Б. Вехов и некоторые другие ученые выделяют два способа перехвата компьютерной информации: активный и пассивный [11, с. 58]. При непосредственном (активном) перехвате злоумышленник осуществляет перехват с помощью непосредственного подключения к телекоммуникационному оборудованию компьютера, системе, сети, например, линии принтера или телефонному проводу канала связи, используемого для передачи данных и управляющих сигналов компьютерной техники. Электромагнитный (пассивный) перехват осуществляется без непосредственного подключения к системе путем фиксации и закрепления на физический носитель электромагнитного излучения, возникающего при функционировании средств компьютерной техники.

Следует отметить, что Конвенция Совета Европы, принятая в 2001 году, содержит отдельную норму о незаконном перехвате компьютерной информации. Так, под перехватом данных понимается преднамеренно осуществленный с использованием технических средств перехват без права на это не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные [6].

Иное неправомерное завладение компьютерной информацией означает получение возможности реализации в отношении ее всех или некоторых полномочий владения, распоряжения или пользования при отсутствии действительного или предполагаемого права на это либо осуществление указанных полномочий помимо установленного порядка, с нарушением регламентирующих его правил. Иное неправомерное завладение компьютерной информацией предполагает использование иных, не связанных с копированием, способов ее получения: неправомерное подключение к компьютерной системе, применение подслушивающих устройств, дистанционное фотографирование, хищение носителей информации и производственных отходов, считывание данных в массивах других пользователей, а равно остаточной информации в памяти системы после выполнения санкционированных запросов. Среди других способов Н.А. Бабий выделяет получение компьютерной информации без согласия владельца (собственника), например, кража, грабеж, либо с их согласия, но против воли (вымогательство).

Статья 289 Модельного УК стран СНГ «Неправомерное завладение компьютерной информацией» содержит 4 части. Таким образом, включает составы преступлений от небольшой тяжести (ч. 1 ст. 289) до особо тяжкого преступления (ч. 4 ст. 289). Данная норма содержит ряд квалифицирующих признаков (применение насилия, группа лиц, организованная группа и др.), которых нет в действующем Уголовном законе. К тому же основной состав, в отличие от статьи 352 УК РБ, является формальным и не предусматривает наступление каких-либо вредных последствий как обязательного признака объективной стороны преступления. Часть 2 статьи 289 Модельного УК предусматривает уголовную ответственность за

принуждение к передаче компьютерной информации под угрозой оглашения позорящих сведений о лице или его близких, предания гласности сведений о таких обстоятельствах, которые потерпевший желает сохранить в тайне, а равно под угрозой применения насилия над лицом или его близкими либо под угрозой уничтожения либо повреждения имущества лица, его близких и других лиц, в ведении или под охраной которых находится эта информация [7]. Представляется, что понятие «иное неправомерное завладение», использованное в диспозиции статьи 352 УК, должно охватывать данные действия. Учитывая специфику предмета неправомерного завладения компьютерной информацией, квалификация данных действий по статье 208 УК (Вымогательство) неправильна.

Рассматривать компьютерную информацию как предмет хищения, на наш взгляд, ошибочно по следующим причинам: *во-первых*, предметом хищения может быть только вещь (имущество) и в некоторых случаях право на имущество или действия имущественного характера; *во-вторых*, сложно определить стоимость «похищенной» информации как обязательного признака предмета хищения в уголовно-правовом понимании; *в-третьих*, в отличие от хищения при неправомерном копировании не происходит изъятие предмета преступления. Кража диска с компьютерной информацией образует состав преступления, предусмотренного статьёй 352 УК, однако это не исключает привлечения виновного к ответственности, например, за мелкое хищение. Ценность компьютерной информации не имеет никакого отношения к ценности носителя данной информации. Таким образом, с позиции уголовного права похитить компьютерную информацию невозможно. Однако В. Хилюта [8] высказывает мнение о допустимости криминализации в рамках борьбы с экономической преступностью действий, направленных на противоправное завладение информацией экономического характера, т.е. именно такой, которая вовлечена в экономический оборот и может подлежать некой оценке, выраженной в денежном (стоимостном) или ином эквиваленте.

Общественно опасные последствия. Состав неправомерного завладения компьютерной информацией сконструирован законодателем как материальный, поэтому общественно опасные последствия являются обязательным признаком объективной стороны преступления, который подлежит установлению. Общественно опасные последствия – это существенный вред, причиненный преступлением объекту, охраняемому уголовным законом.

Вред, причиненный неправомерным завладением компьютерной информацией, часто довольно трудно измерить и оценить, что обусловливается характером объекта уголовно-правовой охраны и особенностями предмета преступления. В связи с этим законодатель в конструкции диспозиции статьи 352 УК РБ использовал оценочную категорию «существенный вред». Такие последствия должны устанавливаться в каждом конкретном случае с учетом всех обстоятельств дела. В случае материального характера его как такового будет оцениваться ущерб на сумму, в 40 и более раз превышающую размер базовой величины. В случае нематериального характера ущерба существенным вредом считается, например, нарушение конституционных прав граждан, значительное ущемление прав и законных интересов органов, организаций и учреждений, создание препятствий их нормальной работе (Н.А. Бабий), разглашение сведений, составляющих государственную тайну (А.Н. Лепехин). Между неправомерным завладением компьютерной информацией и наступлением рассматриваемых последствий должна быть установлена причинная связь.

Наличие или отсутствие общественно опасных последствий при неправомерном завладении компьютерной информацией влияет на решение вопроса о стадии совершенного преступления (моменте его окончания). Данное преступление признается оконченным при условии, что в результате действий виновного наступили вредные последствия в виде существенного вреда.

Согласно статье 10 УК основанием уголовной ответственности является не только совершение виновно запрещенного уголовным законом деяния в виде оконченного преступления, но и приготовление к совершению преступления и покушение на совершение преступления.

Неправомерное завладение компьютерной информацией относится к категории преступлений, не представляющих большой общественной опасности (ст. 12 УК). На основании части 2 статьи 13 УК приготовительные действия к совершению рассматриваемого преступления уголовную ответственность не влекут (однако могут содержать признаки иного преступления или административного проступка).

За умышленные действия, непосредственно направленные на несанкционированное копирование, перехват компьютерной информации или иное неправомерное завладение, если при этом преступление не было доведено до конца по не зависящим от этого лица обстоятельствам (не был причинен существенный вред, не удалось завладеть компьютерной информацией), лицо подлежит уголовной ответственности по части 1 статьи 14 и статье 352 УК.

Заключение. Анализ статистических данных о зарегистрированных в Беларуси преступлениях в сфере высоких технологий за последние 10 лет показал тенденцию постоянного роста количества преступлений данной категории. Однако подобная динамика происходит в основном за счет роста числа хищений путем использования компьютерной техники в общей структуре «высокотехнологичных» преступлений: доля преступлений против информационной безопасности в разные годы составляет 2 – 11 % от общего числа. Еще более незначительное место в общей структуре компьютерных преступлений занимает неправомерное завла-

дение компьютерной информацией: зарегистрировано в 2009 году – 0,009 %; в 2010 – 0,48 %; в 2011 году – 0,14 %. Ошибочно было бы предполагать, что количество преступлений, посягающих на информационную безопасность, уменьшается. Учитывая высочайший уровень латентности, трансграничный характер и постоянное совершенствование способов совершения, выявление и расследование преступлений против информационной безопасности становится все сложнее. Так, в 2009 году направлено в суд уголовных дел по статье 352 УК от числа зарегистрированных преступлений – 100 %, в 2010 году – 58 %, в 2011 году – 67 %. Ошибочная квалификация деяния, подпадающего под признаки неправомерного завладения компьютерной информацией, может привести к отказу в возбуждении уголовного дела, прекращению производства по делу, затягиванию срока расследования. Насыщенность диспозиции статьи 352 УК техническими терминами, которые не имеют официального толкования, оценочный характер общественно опасных последствий данного преступления, отсутствие обобщения судебной практики по уголовным делам о преступлениях против информационной безопасности создают предпосылки неверной квалификации деяний, подпадающих под признаки неправомерного завладения компьютерной информацией.

Нами видятся два варианта выхода из сложившейся ситуации: *во-первых*, принятие Пленумом Верховного суда Постановления о судебной практике по делам о преступлениях против информационной безопасности, дающего разъяснения отдельным терминам и понятиям (компьютерная система, средства компьютерной связи, существенный вред, компьютерная информация и др.), а также обобщающего судебную практику и содержащего особенности квалификации деяний, подпадающих под признаки преступлений против информационной безопасности; *во-вторых*, внесение изменений и дополнений в Закон Республики Беларусь «Об информации, информатизации и защите информации». Уголовному праву Республики Беларусь давно известно использование в Уголовном законе бланкетных норм, которые «отправляют» нас к другим нормативным актам, подробно регламентирующим те или иные общественные отношения.

ЛИТЕРАТУРА

1. Об утверждении Концепции национальной безопасности Республики Беларусь: Указ Президента Респ. Беларусь от 09.11.2010 № 575 // Нац. реестр правовых актов Респ. Беларусь, 18.11.2010. – № 276 1/12080.
2. Бабий, Н.А. Уголовное право Республики Беларусь. Общая часть: учебник / Н.А. Бабий. – Минск: ГИУСТ БГУ, 2010. – 663 с.
3. Научно-практический комментарий к Уголовному кодексу Республики Беларусь / Н.Ф. Ахаменка [и др.]; под ред. А.В. Баркова, В.М. Хомича. – 2-е изд., с изм. и доп. – Минск: ГИУСТ БГУ, 2010. – 1064 с.
4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 07.12.2011) (с изм. и доп. 19.12.2011) // Консультант Плюс: Версия Проф. [Электронный ресурс] / ООО «ЮрСпектр». – Минск, 2011.
5. Научно-практический комментарий к Уголовному кодексу Российской Федерации. Т. 2. – Н.-Новгород, 1996.
6. Convention on Cybercrime. The Council of Europe. Hungary. – 2001 [Электронный ресурс]. – Режим доступа: http://cyber-crime.com/legislative. – Дата доступа: 17.12.2011.
7. Модельный Уголовный кодекс СНГ [Электронный ресурс]. – Режим доступа: http://www.cisatc.org/ /135/154/241. – Дата доступа: 22.02.2012.
8. Хилюта, В. Можно ли похитить информацию? / В. Хилюта // Законность. – 2008. – № 5. – С. 48 – 49.
9. Белорусская юридическая энциклопедия: в 4-х т. Т. 2. К – О; редкол.: С.А. Балашенко [и др.]. – Минск: ГИУСТ БГУ, 2009. – 584 с.
10. Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации, 1 июня 2001 г. // Содружество. Информ. вестн. Совета глав гос-в и Совета глав Правительств СНГ. – № 1. – 2001. – С. 23 – 31.
11. Вехов, В.Б. Компьютерные преступления: способы совершения и методы расследования / В.Б. Вехов; под ред. акад. Б.П.Смагоринского. – М.: Право и закон, 1996. – 182 с.

Поступила 09.08.2012

OBJECTIVE SIGNS OF COMPUTER INFORMATION MISAPPROPRIATION

M. DUBKO

The article deals with penal description of objective signs of computer information misappropriation as a crime against information safety. Particularly the article touches upon features of an object and subject of the crime, as well as elements of a criminal act. Statistical data analysis of crimes in the sphere of high technologies in Belarus shows the tendency of constant growth of the quantity of crimes belonging to the given category. Two options to solve the problem are presented.