УДК 343.534

ОСОБЕННОСТИ КВАЛИФИКАЦИИ НЕПРАВОМЕРНОГО ЗАВЛАДЕНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИЕЙ И ОТГРАНИЧЕНИЯ ОТ ИНЫХ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Рассматриваются отдельные вопросы квалификации неправомерного завладения компьютерной информацией и отграничения данного преступления от других преступлений против информационной безопасности, ряда иных общественно опасных деяний, предметом или средством совершения которых является компьютерная информация. Сформулированы правила квалификации деяний, связанных с неправомерным завладением информацией различных видов (коммерческая тайна, банковская тайна, личная или семейная тайна и др.), которая может быть представлена в виде компьютерной информации, и выделены основные разграничительные признаки составов преступлений, точное установление которых позволит однозначно решить вопрос о юридической оценке таких деяний.

В следственной и судебной практике возникает немало вопросов, связанных с квалификацией преступлений против информационной безопасности, которые становятся все актуальнее в связи с ростом числа преступлений данной категории, появлением новых средств и способов их совершения. Помимо недостаточной разработанности теоретической модели компьютерных преступлений и отсутствия единства в толковании их признаков, влияющих на квалификацию содеянного, определенные трудности при квалификации вызваны наличием в диспозициях данных составов преступлений терминов, которые не имеют однозначного определения и являются специальными. Сложности юридической оценки преступных деяний в сфере информационной безопасности и ошибки, допускаемые в этой связи в правоприменительной практике, не способствуют эффективной борьбе с указанным видом преступлений.

Основная часть. Криминализировав несанкционированный доступ к компьютерной информации (статья 349 Уголовного кодекса Республики Беларусь (УК)) путем закрепления его в статье, «открывающей» главу преступлений против информационной безопасности, законодатель, считает Н.А. Швед, по сути, определил фундамент компьютерных преступлений, сориентированных на признаки состава этого преступления [1, с. 36]. Однако представляется, что несанкционированный доступ к компьютерной информации является более способом обеспечения противоправного воздействия на компьютерную информацию, криминализированного статьями 350–352 УК, и с которым должна связываться повышенная уголовная ответственность. Ввиду этого для обеспечения логичного и последовательного построения норм в главе преступлений против информационной безопасности состав несанкционированного доступа к компьютерной информации должен располагаться после состава неправомерного завладения компьютерной информацией.

Родовой объект всех составов преступлений против информационной безопасности единый, в отличие от непосредственного объекта. При несанкционированном доступе вред причиняется установленному *порядку ознакомления* с информацией и *доступа* к ней. Непосредственным же объектом неправомерного завладения компьютерной информации являются общественные отношения, устанавливающие *порядок получения* компьютерной информации.

Предметом преступлений, предусмотренных статьями 349 и 352 УК, является компьютерная информация. Однако, на наш взгляд, необоснованно не включена в диспозицию статьи 349 УК в качестве предмета преступления информация, *передающаяся* по каналам связи, особенно с учетом широкого распространения беспроводных технологий ее передачи различных видов (например, Wi-Fi, WiMax, EDGE и пр.).

Указанные составы преступлений являются материальными и предусматривают наступление общественно опасных последствий. Вместе с тем в практике в подавляющем большинстве неправомерному завладению с минимальным временным промежутком предшествует несанкционированный доступ. В случае наступления существенного вреда только в результате неправомерного завладения компьютерной информацией и при отсутствии квалифицирующих признаков, предусмотренных частями 2 и 3 статьи 349 УК, состав несанкционированного доступа будет отсутствовать, а деяние подлежит квалификации по статье 352 УК и статье 22.6 Кодекса Республики Беларусь об административных правонарушениях (КоАП). Поэтому для верной квалификации указанных деяний необходимо точно установить, в результате каких конкретно действий наступили предусмотренные диспозицией статей последствия, и причинную связь между ними. При этом считаем, что факт несанкционированного доступа к компьютерной информации автоматически делает последующее завладение компьютерной информацией неправомерным, поэтому установление факта неправомерности последующего завладения информацией не обязательно.

Согласимся с Н.А. Швед в том, что действие, предусмотренное статьей 352 УК, характеризуется определенной направленностью умысла и вряд ли может выступать в качестве последствия несанкционированного доступа [2]. Исключением является автоматическое копирование компьютерной информации в оперативную память компьютера при получении доступа к ней. Однако такое копирование компьютерной информации является автоматическим (неконтролируемым) временным процессом, который носит вспомогательную для работы компьютера функцию. Привлечение к ответственности в таком случае не будет соответствовать принципу субъективного вменения, а само деяние не обладает присущей преступлению степенью общественной опасности, поэтому полагаем, что такое копирование должно оставаться за рамками уголовного закона.

В то же время неправомерное завладение компьютерной информацией и предшествующий ему несанкционированный доступ часто взаимосвязаны между собой и являются результатом реализации единого умысла виновного. Тем не менее диспозиции части 1 статьи 349 и статьи 352 УК требуют наступления существенного вреда в результате каждого из этих деяний, что делает привлечение лица по совокупности преступлений, предусмотренных частью 1 статьи 349 и статьи 352 УК, весьма проблематичным. Это создает условия для необоснованно расширительного толкования органом, ведущим уголовный процесс, признака «иной личной заинтересованности» и квалификации деяния по части 2 статьи 349 и статьи 352 УК.

Учитывая, что необходимым условием копирования и иного завладения компьютерной информацией является получение доступа к данной информации, на наш взгляд, неправомерное завладение компьютерной информацией, сопряженное с несанкционированным доступом, должно рассматриваться в качестве самостоятельного преступления, которое обладает значительно большей общественной опасностью, чем преступление, предусмотренное статьей 352 УК, так как такими действиями дополнительно причиняется вред установленному порядку ознакомления с информацией и доступа к ней, нарушается система защиты информации. Поэтому предлагается включить в статью 352 УК такой *квалифицирующий признак*, как сопряженность завладения компьютерной информацией с несанкционированным доступом. При этом обращаем внимание, что аналогичный квалифицирующий признак содержат составы преступлений, предусмотренные статьями 350 и 351 УК, устанавливающие наряду со статьей 352 УК ответственность за противоправные и общественно опасные формы воздействия на компьютерную информацию.

Основное отличие рассматриваемого преступления от преступления, предусмотренного статьей 350 УК, заключается в признаках объективной стороны состава преступления и непосредственного объекта преступления. Так, непосредственным объектом модификации компьютерной информации выступают общественные отношения, обеспечивающие *целостность* (неизменность) компьютерной информации. Объектом неправомерного завладения являются общественные отношения, обеспечивающие порядок получения информации. В отношении предмета преступления фактически данные действия выражаются в том, что при неправомерном копировании и модификации компьютерная информация не выходит из владения законного собственника (пользователя) – различен лишь характер воздействия на информацию. Исключение составляют случаи неправомерного завладения, связанные с изъятием информации у собственника (пользователя). Особенности объекта неразрывно связаны с признаками противоправного деяния. Так, при несанкционированном копировании и завладении предмет преступления не подвергается изменению, в отличие от модификации, при которой информация подвергается изменению либо в нее вносятся заведомо ложные сведения.

Разграничение противоправных деяний, предусмотренных статьями 351 и 352 УК, необходимо производить по непосредственному объекту и предмету преступления. В отличие от предыдущих составов главы 31 УК, непосредственным предметом деяния, предусмотренного статьей 351 УК, помимо компьютерной информации альтернативно являются компьютерная программа, компьютерное оборудование, компьютерная система, сеть или машинный носитель. Соответственно, непосредственным объектом данного деяния являются общественные отношения, обеспечивающие нормальное функционирование компьютерного оборудования, компьютерных систем, сетей и программ. В отличие от неправомерного завладения, состав компьютерного саботажа является формальным, и наступление последствий в виде существенного вреда диспозицией нормы не предусмотрено, представляется, по причине того, что совершение таких действий *сопряжено* с причинением существенного вреда (по аналогии ч. 1 ст. 349 УК). В случае если после несанкционированного копирования злоумышленником компьютерная информация уничтожается, блокируется, то его действия необходимо квалифицировать по совокупности двух преступлений, предусмотренных статьей 351 УК и статьей 352 УК.

Деяние, предусмотренное статьей 354 УК, фактически является приготовительным действием к неправомерному завладению компьютерной информацией, однако образует специальный состав преступления, в связи с чем такие деяния квалифицируются по совокупности. В то же время за рамками состава преступления, предусмотренного статьей 354 УК, остается разработка компьютерных программ с целью копирования информации, *передаваемой с использованием средств компьютерной связи* – предмета пре-

ступления, предусмотренного статьей 352 УК, а также разработка, использование либо распространение вредоносных программ с целью не только несанкционированного копирования, но и иного неправомерного *завладения* компьютерной информацией. Указанные законодательные пробелы требуют устранения путем корректировки части 1 статьи 354 УК.

Для обеспечения системности правового регулирования в части 1 статьи 354 УК предлагается внести следующие изменение и дополнение:

слова «или копирования» заменить словами «, копирования или иного завладения»;

после слова «носителях,» дополнить словами «или передаваемой с использованием средств компьютерной связи».

В уголовном законе Беларуси имеется целый ряд иных составов преступлений, направленных на уголовно-правовую охрану общественных отношений, связанных с защитой информации определенного вида, которые содержатся в различных главах УК. В связи с этим определенные трудности на практике может вызывать отграничение состава преступления, предусмотренного статьей 352 УК, от иных составов, в которых компьютерная информация выступает предметом или средством совершения преступления.

В указанном случае, полагаем, следует руководствоваться принципом квалификации преступлений при конкуренции норм. Как отмечает В.Н. Кудрявцев, общая черта норм, находящихся в конкуренции, состоит в том, что они с разной степенью обобщения и с различной полнотой предусматривают признаки одного и того же преступления, и, следовательно, как по объекту, так и по содержанию эти нормы частично совпадают [3]. Однако при детальном анализе одна из них будет являться специальной по отношению к другой. Правило квалификации в таких случаях определено частью 2 статьи 42 УК.

В случаях, пишет В.В. Марчук, когда сложность и запутанность в конструкции уголовно-правовых норм допускает различные варианты квалификации преступления, следует решать вопрос о приоритете в принятии решения относительно квалификации на основе сложившихся представлений о справедливости [12, с. 165]. К распределяющему аспекту принципа социальной справедливости (индивидуализация наказания) при квалификации преступлений ученый относит положение части 6 статьи 3 УК о том, что никто не может нести дважды уголовную ответственность за одно и то же преступление, или «недопустимость двойного инкриминирования».

При неправомерном завладении компьютерной информацией предметом преступления является компьютерная информация, не имеющая физических характеристик и одновременно неразрывно связанная с компьютером, компьютерной системой, машинным носителем. Поэтому завладение компьютерной информацией часто совершается путем противоправного завладения ее носителем (жесткого диска компьютера, flash-карты памяти, компакт-диска). В данном случае можно вести речь об идеальной совокупности преступлений, когда одним деянием вред причиняется двум объектам – отношениям по обеспечению безопасности компьютерной информации и отношениям собственности, которые образуют самостоятельные составы преступлений. В этой связи помимо статьи 352 УК необходима дополнительная квалификация по соответствующим статьям главы 24 УК в зависимости от способа хищения носителя компьютерной информации.

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. Как справедливо отмечается С. Овсейко, термин «право собственности» применительно к информации неуместен и может использоваться в отсутствие иной терминологии не более чем юридическая фикция [4, с. 59]. Схожей позиции придерживается Л.К. Терещенко, утверждая, что классическая «триада» правомочий собственника, обладающего абсолютным правом на вещь, не применима в отношении информации [10, с. 4]. В этой связи поддерживаем мнение О.С. Кашининой о том, что необходимо исходить из определения информации как самостоятельного объекта гражданских прав, *отличного от имущества* [13, с. 133].

Кража компакт-диска с компьютерной информацией образует состав преступления, предусмотренного статьей 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.В. Хилюта высказывает мнение о допустимости криминализации в рамках борьбы с экономической преступностью действий, направленных на противоправное завладение информацией экономического характера, то есть именно такой, которая вовлечена в экономический оборот и может подлежать некой оценке, выраженной в денежном (стоимостном) или ином эквиваленте [5, с. 49].

Согласно данным Министерства внутренних дел Республики Беларусь в структуре высокотехнологичных преступлений подавляющее большинство (более 90%) занимают хищения путем использова-

ния компьютерной техники (ст. 212 УК), число которых ежегодно увеличивается. Поэтому актуальным является вопрос отграничения данного преступления от преступлений против информационной безопасности, в частности от неправомерного завладения компьютерной информацией.

Непосредственным объектом преступления, предусмотренного статьей 212 УК, являются отношения собственности, а предметом – имущество. В отличие от неправомерного завладения компьютерной информацией, информация, обрабатываемая в компьютерной системе, хранящаяся на машинных носителях или передаваемая по сетям передачи данных, является не предметом, а средством совершения хищения. Например, при хищении денежных средств с карт-счета используется как компьютерная техника (скимеры, шимы, накладки на цифровую панель), так и компьютерная информация – реквизиты банковской платежной карты (номер карты, пин-код). Общественные отношения по обеспечению установленного порядка ознакомления и работы с компьютерной информацией являются дополнительным объектом квалифицированного состава (ч. 2 ст. 212 УК).

В ряде ситуаций лицо с целью совершения хищения на этапе подготовки или непосредственного совершения преступления может неправомерно завладеть компьютерной информацией [6]. Указанные действия образуют простую или идеальную *совокупность преступлений*. Так, без реквизитов банковской платежной карты, которые содержатся на магнитной полосе карты либо чипе и относятся к категории компьютерной информации, невозможно изготовить поддельную банковскую карту, а без пин-кода войти в систему банкомата, тем самым осуществив несанкционированный доступ, и произвести операции по карт-счету держателя карты (перевод, снятие наличных денежных средств). Таким образом, в случае завладения компьютерной информацией (при наступлении существенного вреда в результате такого завладения) и последующем хищении имеет место совокупность двух преступлений, предусмотренных статьей 212 УК и статьей 352 УК.

Пленум Верховного Суда Республики Беларусь дал разъяснение, в соответствии с которым «... хищение путем использования компьютерной техники, сопряженное с несанкционированным доступом к компьютерной информации, сопровождавшимся наступлением последствий, указанных в статье 349 УК, квалифицируется по совокупности преступлений (ч. 2 ст. 212 и ч. 2 или 3 ст. 349 УК)» [7]. Полагаем, что по аналогии подлежат квалификации и действия лица, когда оно с целью последующего совершения хищения на этапе подготовки или совершения преступления неправомерно завладевает компьютерной информацией.

Учитывая изложенное, представляет интерес следующий *пример из судебной практики*. Так, при рассмотрении уголовного дела по обвинению П. в совершении преступлений, предусмотренных статьей 14 и частью 4 статьи 212, частью 3 статьи 212, статьей 13 и частью 2 статьи 212, частью 1 статьи 222, частью 2 статьи 222, частью 2 статьи 349, частью 2 статьи 17 и статьи 352, статьей 14 и статьей 353 УК, суд пришел к выводу о необходимости исключения из обвинения по статье 352 УК излишне указанное несанкционированное копирование информации с не принадлежащих П. банковских платежных карт (*авт.* реквизиты которых он в последующем использовал для изготовления поддельных банковских карт и похитил денежные средства держателей этих карт), поскольку действия обвиняемого охватываются составами преступлений, предусмотренными частью 1 статьи 14 и частью 4 статьи 212, частью 3 статьи 212, частью 1 статьи 13 и частью 2 статьи 212 УК.

Суд также пришел к убеждению об излишнем вменении в вину П. части 2 статьи 349 УК, поскольку содеянное обвиняемым в части использования скомпрометированных реквизитов банковских платежных карт при совершении хищений, предусмотренных частью 1 статьи 14 и частью 4 статьи 212, частью 3 статьи 212, частью 1 статьи 13 и частью 2 статьи 212 УК, подпадает под квалификацию по названным статьям, а в части оставшихся неиспользованными реквизитов карт либо использованных, но по которым обвиняемый отказался проводить операции после успешного просмотра баланса, действия лица подлежат квалификации по статье 352 УК, в связи с чем исключил ее [8].

Подход суда в данном случае видится недостаточно необоснованным, так как вменение лицу факта неправомерного завладения компьютерной информацией не должно ставиться в зависимость от последующего использования (неиспользования) данной информации в преступных целях. Хищение путем использования компьютерной техники и неправомерное завладение компьютерной информацией являются самостоятельными и не взаимоисключающими преступлениями.

Актуальным является вопрос квалификации деяний, связанных с завладением различного рода информацией, которая может быть представлена в виде компьютерной информации. В комментарии к УК указывается, что в случае завладения коммерческой тайной, которая одновременно является компьютерной информацией, требуется дополнительная квалификация содеянного по статьям о преступлениях против информационной безопасности [9, с. 579]. Представляется, что дополнительная квалификация по статье 352 УК в данном случае не требуется, так как статья 254 УК является специальной по отношению к последней – посягательство осуществляется на общественные отношения, устанавливающие порядок

обращения и обеспечивающие конфиденциальность коммерческой тайны, а предметом преступления являются сведения, составляющие коммерческую тайну.

Такого же подхода необходимо придерживаться в случае неправомерного завладения сведениями, составляющими банковскую тайну, которые хранятся на машинном носителе компьютера или системы либо передаются по каналам связи. Так, обязательным признаком деяния, предусмотренного частью 1 статьи 254 УК, является цель – незаконное использование информации (банковской тайны). Поэтому при неправомерном завладении сведениями, составляющими банковскою тайну, которые хранятся или обрабатываются на компьютере или машинном носителе, с целью последующего хищения денежных средств, в соответствии с требованиями части 2 статьи 42 УК должна применяться часть 1 статьи 254 УК как более полно охватывающая признаки совершенного деяния и являющаяся специальной по отношению к статье 352 УК. При этом необходимо отметить, что часть 1 статьи 254 УК предусматривает наказание в виде лишения свободы до трех лет (менее тяжкое преступление), в то время как статья 352 УК – до двух лет (преступление, не представляющее большой общественной опасности).

Статья 179 УК предусматривает ответственность за незаконное собирание либо распространение сведений о частной жизни, составляющих личную или семейную тайну другого лица, без его согласия, повлекшие причинение вреда правам, свободам и законным интересам потерпевшего. Фактически данный состав предусматривает ответственность за завладение информацией, распространение которой ограничено, повлекшее причинение существенного вреда. Частью 2 данной статьи криминализировано то же действие, совершенное с использованием специальных технических средств, предназначенных для негласного получения информации. При завладении лицом информацией о частной жизни, составляющей личную или семейную тайну другого лица в электронном виде, возникает конкуренция между статьями 179 и 352 УК. При квалификации необходимо, прежде всего, исходить из особенностей объекта и предмета совершенного преступления и направленности умысла. Применяться в таком случае должна специальная норма, то есть статья 179 УК. При этом полагаем, что обычные пользовательские компьютеры не могут относиться к специальным средствам, в связи с чем квалификация по части 2 статьи 179 УК исключается.

Аналогичный подход необходимо использовать при отграничении неправомерного завладения компьютерной информацией от незаконного нарушения тайны переписки, телефонных или иных переговоров, почтовых, телеграфных или иных сообщений граждан (ст. 203 УК), похищения либо собирания незаконным способом сведений, составляющих коммерческую или банковскую тайну, с целью их разглашения либо незаконного использования (ст. 254 УК), похищения, собирания с целью передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну (ст. 358 УК), хищении официальных документов (ст. 377).

Заключение. Резюмируя, отметим, что сходными по объективной стороне с составом преступления, предусмотренным статьей 352 УК, являются некоторые иные деяния, если они совершаются путем неправомерного завладения компьютерной информацией [11, с. 19]. Разграничение, в первую очередь, необходимо производить по предмету посягательства. Так, если предмет – компьютерная информация, содержащая определенные сведения, завладение которыми образует состав самостоятельного преступления, содеянное необходимо квалифицировать только как это преступление (без дополнительной квалификации по ст. 352 УК). Если же предметом является иная компьютерная информация, то деяние следует квалифицировать как неправомерное завладение ею по статье 352 УК. Немаловажное значение имеет также анализ субъективной стороны, установление мотивов и целей, которыми руководствовался виновный. Приготовление к хищению (например, вымогательству), разглашению тайны усыновления, нарушению авторских, смежных, изобретательских и патентных прав, умышленному разглашению государственной тайны, разглашению коммерческой тайны и к некоторым другим преступлениям также может быть совершено путем завладения компьютерной информацией. В данном случае действия по завладению компьютерной информацией подлежат самостоятельной оценке, а содеянное в указанных случаях следует квалифицировать по совокупности преступлений – по статье 352 УК и как приготовление к конкретному преступлению.

На основе изложенного и опираясь на анализ следственной и судебной практики можно констатировать, что неправомерные действия лица в отношении компьютерной информации часто не охватываются рамками одной статьи главы 31 УК, а квалифицируются по нескольким ее статьям. Смежные составы преступлений против информационной безопасности схожи по характеру общественной опасности и различаются по одному или нескольким признакам – в основном это элементы объективной стороны, характеризующие способ негативного воздействия на компьютерную информацию.

Если несанкционированное завладение компьютерной информацией выступает в качестве способа совершения иных преступлений либо совершается в процессе приготовительных действий или в процессе совершения преступления, имеет место совокупность преступлений. При завладении компьютерной информацией, ответственность за неправомерное получение которой предусмотрена специальной нормой УК, квалификация осуществляется по специальной норме. Среди основных разграничительных при-

знаков выступают особенности предмета преступления и, соответственно, объекта преступления, цели и мотивы совершения деяния, характер причиненного вреда (ущерба), точное установление которых позволит однозначно решать вопрос квалификации неправомерного завладения компьютерной информацией.

ЛИТЕРАТУРА

1. Швед, Н.А. Несанкционированный доступ к компьютерной информации: оптимизация уголовной ответственности / Н.А. Швед // Юридический мир. – 2009. – № 12. – С. 36–41.
2. Швед, Н.А. Уголовная ответственность за несанкционированный доступ к компьютерной информации: дис. ... канд. юрид. наук: 12.00.08 / Н.А. Швед. – Минск, 2010. – 166 с.
3. Кудрявцев, В.Н. Общая теория квалификации преступлений / В.Н. Кудрявцев. – М., 1999. – С. 211.
4. Овсейко, С. Информация как объект права: понятие, передача, защита / С. Овсейко // Юстыцыя Беларусі. – 2014. – № 3. – С. 55–60.
5. Хилюта, В.В. Можно ли похитить информацию? / В.В. Хилюта // Законность. – 2008. – № 5. – С. 48–49.
6. Хилюта, В.В. Отграничение состава преступления, предусмотренного статьей 212 Уголовного кодекса Республики Беларусь от иных составов преступлений / В.В. Хилюта [Электронный ресурс]. – СПС «КонсультатнПлюс Беларусь», 2015.
7. О применении судами уголовного законодательства по делам о хищениях имущества: постановление Пленума Верховного Суда Республики Беларусь от 21 дек. 2001 г. № 15 (в ред. от 24.09.2009) [Электронный ресурс]. – СПС «КонсультатнПлюс Беларусь», 2015.
8. Уголовное дело по обвинению П. в совершении преступлений, предусмотренных ст. 14 и ч. 4 ст. 212, ч. 3 ст. 212, ст. 13 и ч. 2 ст. 212, ч. 1 ст. 222, ч. 2 ст. 222, ч. 2 ст. 349, ч. 2 ст. 17 и ст. 352, ст. 14 и ст. 353 УК // Архив суда Железнодорожного района г. Витебска.
9. 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.
10. Терещенко, Л.К. Информация и собственность / Л.К. Терещенко // Защита прав создателей и пользователей программ для ЭВМ и баз данных (комментарий к российскому законодательству). – М., 1996. – С. 3–6
11. Лосев, В. Уголовно-правовой анализ преступлений против информационной безопасности / В. Лосев // Судовы веснік, 2003. – № 4. – С. 18–22.
12. Марчук, В.В. Теория квалификации преступления / В.В. Марчук; Акад. МВД Респ. Беларусь. – Минск: Акад. МВД, 2014. – 339 с.
13. Каширина, О.С. Состояние и направления совершенствования законодательства Республики Беларусь в сфере информации, информатизации и защиты информации / О.С. Каширина // Проблемы правовой информатизации. – 2007. – № 2. – С. 133.

Поступила 03.09.2015

FEATURES OF QUALIFICATION OF THE COMPUTER INFORMATION MISAPPROPRIATION AND DELIMITATION FROM OTHER CRIMES AGAINST INFORMATION SECURITY

M. DUBKO

The article discusses some questions of qualification of the computer information misappropriation, such as delimitation this crime from other crimes against information security and socially dangerous acts or means of the subject which is information.