БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УДК 343.534(476)(043.3)

ДУБКО
Михаил Анатольевич

НЕПРАВОМЕРНОЕ ЗАВЛАДЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИЕЙ КАК ПРЕСТУПЛЕНИЕ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Автореферат диссертации на соискание ученой степени
кандидата юридических наук

по специальности 12.00.08 – уголовное право и криминология;
уголовно-исполнительное право

Минск, 2018

Научная работа выполнена в Белорусском государственном университете

Научный руководитель	**Шевцов Юрий Леонидович,** кандидат юридических наук, доцент, заместитель декана юридического факультета Белорусского государственного университета
Официальные оппоненты:	**Савенок Анатолий Леонидович,** доктор юридических наук, доцент, заведующий кафедрой уголовного права и криминологии учреждения образования «Академия Министерства внутренних дел Республики Беларусь»;
	Лапцевич Ирина Игоревна, кандидат юридических наук, начальник отдела исследований в области правоохранительной деятельности и осуществления правосудия Института правовых исследований Национального центра законодательства и правовых исследований Республики Беларусь
Оппонирующая организация	**Академия управления при Президенте Республики Беларусь**

Защита состоится 11 декабря 2018 года в 15:00 часов на заседании совета по защите диссертаций Д 02.01.04 при Белорусском государственном университете по адресу: 220030, г. Минск, ул. Ленинградская, 8, аудитория 407, тел. 226-55-41.

С диссертацией можно ознакомиться в библиотеке Белорусского государственного университета.

Автореферат разослан «___» ноября 2018 года.

Ученый секретарь
совета по защите диссертаций
кандидат юридических наук, доцент А.В. Шидловский

ВВЕДЕНИЕ

Развитие информационного общества в республике является одним из национальных приоритетов. Вопросы защиты компьютерной информации приобрели особую актуальность в рамках реализации Программы социально-экономического развития Республики Беларусь на 2016–2020 гг., Государственной программы инновационного развития Республики Беларусь на 2016–2020 гг., а также Декрета Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики». В данных условиях роль и значение общественных отношений, связанных с оборотом компьютерной информации, существенно возросли, а информационная безопасность стала важнейшей составляющей национальной безопасности государства в целом.

Социальная опасность преступлений против информационной безопасности обусловлена широким применением в республике систем безналичных расчетов, развитием цифровой экономики и электронного правительства, автоматизацией производств, созданием республиканских и ведомственных информационных систем, нормальное функционирование которых может быть нарушено путем деструктивного воздействия на компьютерную информацию. К одному из таких общественно опасных деяний, посягающих на информационную безопасность, законодатель отнес неправомерное завладение компьютерной информацией (ст. 352 УК).

Недостаточная исследованность признаков указанного состава преступления, его места в системе уголовного закона, особенности законодательной конструкции статьи, неединообразная правоприменительная практика в совокупности создают трудности при производстве по материалам и уголовным делам о таких преступлениях, количество которых ежегодно возрастает. Отдельные вопросы уголовной ответственности за преступления против информационной безопасности рассматривались в работах таких белорусских ученых, как Н.Ф. Ахраменка, И.О. Грунтов, Г.А. Зорин, В.Е. Козлов, Д.Н. Лабоцкий, А.П. Леонов, А.Н. Лепехин, В.В. Лосев, Э.Ф. Мичулис, Д.Г. Мороз, А.Л. Савенок, В.В. Хилюта, В.Н. Черкасов, Н.А. Швед и др. Однако уголовно-правовые аспекты противодействия неправомерному завладению компьютерной информацией в исследованиях белорусских ученых не нашли достаточного отражения и не позволяют в полной мере разрешать возникающие на практике проблемы. Изложенное предопределяет актуальность избранной темы с теоретической и практической стороны.

Научно-практическая значимость диссертации состоит в разработке и обосновании теоретических положений уголовно-правовой регламентации ответственности за неправомерное завладение компьютерной информацией, предложений по совершенствованию уголовного закона и рекомендаций по формированию единообразной практики его применения.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с научными программами (проектами), темами

Настоящее исследование является частью проводимых на кафедре уголовного права юридического факультета Белорусского государственного университета научно-исследовательских работ по теме «Совершенствование правового регулирования и механизмов функционирования системы противодействия преступности, защиты прав и свобод человека» подпрограммы «Теоретико-методологические основы совершенствования национальной правовой системы и управления в контексте социально-экономического развития Республики Беларусь» Государственной программы научных исследований на 2011–2015 гг. «Гуманитарные науки как фактор развития белорусского общества и государственной идеологии» (ГПНИ «История, культура, общество, государство»), утвержденной постановлением Совета Министров Республики Беларусь от 9 июня 2010 г. № 886 (№ госрегистрации 20115607), а также теме «Тенденции развития уголовного и уголовно-исполнительного законодательства и совершенствование правоприменительной практики в современных условиях» подпрограммы «Правовые и организационные механизмы воздействия на преступность и правонарушения в контексте защиты национальных интересов и иных приоритетов современной правоохранительной политики» Государственной программы научных исследований на 2016–2020 гг. (ГНПИ «Экономика и гуманитарное развитие белорусского общества»), утвержденной постановлением Совета Министров Республики Беларусь от 10 июня 2015 г. № 483 (№ госрегистрации 20161833).

Тема диссертации соответствует подп. 11.4 и п. 13 перечня приоритетных направлений научных исследований Республики Беларусь на 2011–2015 гг., утвержденного постановлением Совета Министров Республики Беларусь от 19 апреля 2010 г. № 585, а также п. 245, 250 и 468 перечня актуальных направлений диссертационных исследований в области права на 2012–2016 гг., одобренного решением межведомственного совета по проблемам диссертационных исследований в области права от 5 сентября 2012 г.

Тема исследования также согласуется с п. 54 Концепции национальной

безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, подп. 37.2 мероприятий Программы по борьбе с преступностью и коррупцией на 2013–2015 гг., утвержденной Решением республиканского координационного совещания от 15.03.2013 № 26-07ркс-2013, и п. 2 плана мероприятий Генеральной прокуратуры Республики Беларусь, Следственного комитета Республики Беларусь, Министерства внутренних дел Республики Беларусь по реализации поручений, изложенных в докладной записке Администрации Президента Республики Беларусь от 06.04.2015 «Об эффективности деятельности правоохранительных органов», утвержденного Генеральным прокурором Республики Беларусь 12 июня 2015 г.

Цель и задачи исследования

Целью исследования является разработка теоретических положений уголовной ответственности за неправомерное завладение компьютерной информацией и выработка предложений по совершенствованию уголовного закона и практики его применения в данной части.

Основные *задачи* исследования заключаются в следующем:

проанализировать историческое развитие национального законодательства и теоретических исследований в области защиты компьютерной информации и борьбы с преступлениями против информационной безопасности;

изучить и провести сравнительно-правовой анализ зарубежного опыта уголовно-правовой борьбы с неправомерным завладением компьютерной информацией;

определить основание и причины криминализации неправомерного завладения компьютерной информацией;

провести юридический анализ объективных и субъективных признаков состава преступления, предусмотренного ст. 352 УК;

установить соотношение неправомерного завладения компьютерной информацией с другими преступлениями против информационной безопасности и иными смежными преступлениями, определить особенности их квалификации;

обобщить и проанализировать существующую следственную и судебную практику применения ст. 352 УК, выявить проблемные вопросы практики применения и законодательной конструкции состава неправомерного завладения компьютерной информацией;

сформулировать научно обоснованные рекомендации по совершенствованию правового регулирования ответственности

за неправомерное завладение компьютерной информацией и правоприменительной практики.

Объектом исследования являются общественные отношения, складывающиеся в связи с нарушением уголовно-правовой охраны компьютерной информации посредством неправомерного завладения. *Предмет* исследования составляют нормы уголовного закона, предусматривающие ответственность за неправомерное завладение компьютерной информацией, практика их применения, в том числе статистические данные и материалы 60 уголовных дел, международные правовые акты, законодательство Республики Беларусь и зарубежных стран в области обеспечения информационной безопасности, научные публикации по теме исследования, результаты социологического опроса 172 сотрудников Следственного комитета и прокурорских работников.

Научная новизна

Научная новизна диссертации заключается в том, что автором впервые в республике проведено исследование вопросов уголовно-правовой регламентации ответственности за неправомерное завладение компьютерной информацией. Сформулированные в диссертации научные положения и выводы направлены на обеспечение эффективности норм уголовного закона об ответственности за данное общественно опасное деяние, а также содержат рекомендации по совершенствованию и формированию единообразной практики их применения.

Положения, выносимые на защиту

1. Авторская модель уголовно-правовой регламентации деяний, связанных с противоправным получением (собиранием, похищением, копированием, завладением, перехватом) компьютерной информации, основанная на совокупности следующих положений:

1) при установлении уголовной ответственности за деяния, связанные с противоправным получением информации, в том числе компьютерной, основными критериями криминализации должны выступать содержание информации, являющейся предметом преступления (различные виды охраняемых уголовным законом тайн), и, соответственно, установленный в отношении информации правовой режим. Общественная опасность таких деяний обусловливается причинением (возможностью причинения) существенного вреда в результате неправомерного обладания данной информацией, включая последующее ее использование (разглашение), и не может определяться только формой представления информации;

2) установление в гл. 31 УК уголовной ответственности только за такие способы противоправного получения компьютерной информации, которые сопряжены с причинением существенного вреда исходя из компьютерной формы представления информации, являющейся предметом преступления.

2. С учетом содержания родового объекта состава неправомерного завладения компьютерной информацией, к которому отнесены общественные отношения по обеспечению безопасности компьютерной информации, а также предмета данного преступления, в качестве которого может выступать общедоступная информация и информация, распространение и (или) предоставление которой ограничено, определено основание установления в ст. 352 УК самостоятельной уголовной ответственности за данное деяние. Таковым является общественная опасность деяния, выражающаяся в его свойстве причинить существенный вред охраняемым уголовным законом отношениям независимо от установленного в отношении компьютерной информации, являющейся предметом преступления, правового режима (банковская или коммерческая тайна, тайна личной жизни и др.).

3. Совокупность признаков несанкционированного копирования компьютерной информации, которая обусловливает особенности уголовно-правовой регламентации ответственности за совершение данного деяния в сравнении с существующими в национальном уголовном законодательстве и уголовном законодательстве государств-участников СНГ подходами к его криминализации. Определено, что непосредственным объектом несанкционированного копирования компьютерной информации в отличие от иного неправомерного завладения компьютерной информацией выступают общественные отношения по обеспечению конфиденциальности (неизвестности) информации, а общественную опасность данного деяния альтернативно обусловливают следующие факторы: установленный законодательством в отношении информации правовой режим (например, отнесение информации к государственным секретам, банковской, коммерческой тайне); цель, преследуемая виновным при копировании компьютерной информации (например, последующее совершение преступления с использованием информации); субъективная оценка характера и степени причиненного обладателю информации вреда в зависимости от важности (ценности) для него информации.

4. Предложения по совершенствованию норм об ответственности за неправомерное завладение компьютерной информацией, которые обосновывают необходимость:

4.1 дифференциации уголовной ответственности за перечисленные в ст. 352 УК деяния (несанкционированное копирование, иное неправомерное

завладение) путем исключения из статьи несанкционированного копирования компьютерной информации как одного из способов неправомерного завладения компьютерной информацией. Обосновывается целесообразность сохранения в ст. 352 УК ответственности только за завладение компьютерной информацией, под которым предлагается понимать умышленные действия виновного лица по получению компьютерной информации, в том числе путем перехвата, в результате которых обладатель информации либо ее получатель лишаются возможности использовать данную информацию, то есть действия и их результат, связанные с изъятием информации у обладателя. Реализация данного предложения не повлечет возникновение пробела в правовом регулировании;

4.2 унификации законодательной конструкции уголовно-правовых норм гл. 31 УК, предусматривающих ответственность за компьютерный саботаж, модификацию компьютерной информации и неправомерное завладение компьютерной информацией. Ввиду однородности характера противоправного поведения, близкой степени общественной опасности, отсутствия четких разграничительных признаков между завладением, уничтожением, блокированием, модификацией компьютерной информации предлагается рассматривать их как равнозначные способы посягательства на безопасность компьютерной информации. В этой связи аргументируется изложение ст. 350–352 УК в новой редакции, предусматривающей их сходную структуру (материальная конструкция состава, идентичные квалифицирующие признаки), равный диапазон видов и размера наказаний;

4.3 установления повышенной ответственности за противоправное получение компьютерной информации путем дополнения составов преступлений, предусматривающих ответственность за противоправное получение сведений безотносительно формы их представления, таким квалифицирующим признаком, как «сопряженность с несанкционированным доступом к компьютерной информации, компьютерной системе или сети». Данный квалифицирующий признак одновременно указывает на особенности предмета преступления (компьютерную информацию) и отражает значительное увеличение степени общественной опасности запрещаемого деяния в сравнении с деянием, предусмотренным основным составом.

5. Рекомендации по квалификации деяний, связанных с противоправным получением компьютерной информации. При юридической оценке указанных деяний предлагается руководствоваться следующими правилами:

признание неправомерного завладения компьютерной информацией в качестве преступления, предусмотренного ст. 352 УК, не должно ставиться

в зависимость от последующего использования (неиспользования) данной информации в преступных целях;

действия, выражающиеся в противоправном получении компьютерной информации с целью совершения конкретного преступления (менее тяжкого, тяжкого или особо тяжкого), наряду с приготовлением к его совершению должны получать самостоятельную уголовно-правовую оценку по соответствующим статьям уголовного закона, предусматривающим ответственность за противоправное получение информации;

если неправомерное завладение компьютерной информацией выступает в качестве способа совершения иного преступления, имеет место совокупность преступления, предусмотренного ст. 352 УК, и соответствующего преступления, способом которого явилось неправомерное завладение компьютерной информацией.

Личный вклад соискателя ученой степени

Диссертационная работа представляет собой самостоятельно проведенное исследование избранной темы, заключающееся в непосредственном изучении и систематизации имеющегося по теме исследования научного и практического материала, внесении конкретных предложений по совершенствованию законодательства и практики его применения в части уголовной ответственности за неправомерное завладение компьютерной информацией. Личный вклад соискателя подтверждается также личным участием в апробации результатов исследования в ходе научных и научно-практических конференций, подготовке научных публикаций по теме исследования.

Апробация диссертации и информация об использовании ее результатов

Основные результаты исследования докладывались и обсуждались на заседаниях кафедры уголовного права Белорусского государственного университета в 2012–2018 гг., а также в ходе выступлений на международных, республиканских научных и научно-практических конференциях, круглых столах, в том числе: «Интеграционные экономико-правовые направления развития Украины и стран ближнего зарубежья» (Украина, г. Львов, 31 января 2012 г.), «European and National context in research» (г. Новополоцк, 25–26 апреля 2012 г.), «Современные тенденции развития юридической науки, правового образования и воспитания» (г. Полоцк, 18–19 мая 2012 г.), «Юридическая наука и правоприменительная практика» (г. Минск, 26–27 октября 2012 г.), «Развитие информатизации и государственной системы научно-технической информации (РИНТИ)» (г. Минск, 15 ноября 2012 г.), «Преступления в информационной сфере: проблемы расследования,

квалификации, реализации ответственности и предупреждения» (г. Тамбов, 14–15 февраля 2013 г.), «Людина, суспільство, держава: правовий вимір в сучасному світі» (г. Киев, 27 февраля 2014 г.), «Правотворчество и правоприменение в условиях инновационного развития общества» (г. Гродно, 27–28 февраля 2014 г.), «Социально-психологические аспекты обеспечения национальной безопасности» (г. Минск, 3–4 декабря 2015 г.), «Теоретические и прикладные аспекты современной юридической науки» (г. Минск, 11 декабря 2015 г.), «Проблемы борьбы с преступностью и подготовки кадров для правоохранительных органов» (г. Минск, 10 февраля 2017 г.), «Принципы уголовного права в контексте реализации и защиты прав человека» (г. Минск, 5 июня 2018 г.).

Апробация диссертации также подтверждается внедрением полученных результатов исследования в практическую деятельность правоохранительных и иных государственных органов Республики Беларусь и Российской Федерации, образовательный процесс ведущих учреждений образования.

Опубликование результатов диссертации

Основные положения и результаты исследования отражены в 28 опубликованных научных работах общим объемом 12,6 авторского листа. Из них 10 научных статей объемом 5,3 авторского листа размещены в журналах и сборниках, включенных в Перечень научных изданий Республики Беларусь для опубликования результатов диссертационных исследований; 11 публикаций объемом 2,5 авторского листа – в сборниках материалов научно-практических конференций; 7 статей объемом 4,8 авторского листа – в сборниках научных трудов, информационно-практических изданиях, электронных правовых системах и ресурсах.

Структура и объем диссертации

Структура и объем диссертации определяются целями и задачами исследования. Диссертация выполнена на 224 страницах и состоит из введения, трех глав, объединяющих девять разделов, заключения, библиографического списка, включающего 355 наименований, и приложений. Объем работы без учета библиографического списка и приложений составляет 151 страницу.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Первая глава ***«Социально-правовые причины криминализации неправомерного завладения компьютерной информацией и зарубежный опыт уголовно-правовой борьбы с ним»*** состоит из трех разделов. *Первый раздел «Аналитический обзор литературы по теме диссертации»* посвящен анализу научной литературы по теме исследования. Теоретическую основу

диссертации составили научные труды белорусских и зарубежных ученых в области философии, уголовного права, криминалистики, криминологии, информационного права и иных наук. При рассмотрении общих положений уголовного права автор опирался на труды Н.А. Бабия, А.В. Баркова, И.О. Грунтова, В.Н. Кудрявцева, А.В. Наумова, А.И. Рарога, А.Л. Савенка, Э.А. Саркисовой, Н.С. Таганцева, В.М. Хомича и др.

Анализ научных источников позволил выделить направления развития теоретико-правовых исследований по проблемам преступности в сфере информационной безопасности, а также этапы развития белорусской юридической науки в области уголовно-правового обеспечения информационной безопасности. Отмечено, что в Республике Беларусь и иных постсоветских государствах вопросы правового регулирования новых общественных отношений получили свою актуальность лишь в 90-х годах прошлого столетия. В данный период учеными обосновывается необходимость криминализации ряда деяний в данной сфере. Подчеркивается, что представителями белорусской уголовно-правовой науки до принятия УК не высказывались предложения в части установления уголовной ответственности за неправомерное завладение компьютерной информацией.

Особое внимание автором уделено научным работам Н.Ф. Ахраменка, В.Е. Козлова, А.П. Леонова, В.В. Лосева, А.Н. Лепехина, А.В. Макаревича, Н.А. Швед, положения которых послужили основой проведенного исследования. Автор приходит к выводу об отсутствии в научной литературе единых подходов в понимании сущности преступлений против информационной безопасности, их видов и признаков, иных правовых аспектов данного феномена. Констатируется, что большинство научных работ в данной сфере касается состава несанкционированного доступа к компьютерной информации, в то время как иные составы, включая неправомерное завладение компьютерной информацией, мало исследованы.

Второй раздел «Правовые и социальные причины установления в Республике Беларусь уголовной ответственности за неправомерное завладение компьютерной информацией» посвящен исследованию основания и причин криминализации неправомерного завладения компьютерной информацией. По результатам ретроспективного анализа национального информационного законодательства автором сделан вывод о том, что включение в уголовный закон статей, предусматривающих ответственность за преступления против информационной безопасности, обусловлено в большей степени тенденциями международного и зарубежного законодательства, стремительным развитием в республике сферы информационно-коммуникационных технологий. Отсутствие в системе

законодательства нормативного правового акта, регламентирующего процесс создания, распространения, использования, хранения и уничтожения компьютерной информации, по мнению автора, свидетельствует о незавершенности этапа закрепления уголовной ответственности за преступления против информационной безопасности.

Комплексное рассмотрение национального законодательства, научных работ в области уголовного и информационного права позволяет сделать вывод, что правовой режим той или иной информации обусловливается характером сведений, которые содержит информация, и возможностью наступления негативных последствий ее свободного оборота, а не объективной формой ее представления. Подчеркивается, что исходя из указанных положений выстраивалась система уголовно-правовых норм, предусматривающих ответственность за так называемые информационные преступления в ранее действовавшем УК 1960 г. (ст. 61, 62, 72–73, 122-1, 135, 138, 248 и др.), УК 1999 г. (ст. 177–179, 203, 254, 358, 407 и др.). С учетом данных обстоятельств выделение законодателем неправомерного завладения компьютерной информацией в качестве самостоятельного преступления позволило автору установить основание криминализации данного деяния, что поспособствовало разрешению проблемных вопросов определения конструктивных признаков состава преступления, предусмотренного ст. 352 УК, его юридической оценки и отграничения от смежных составов.

В третьем разделе «Уголовное законодательство зарубежных государств в сфере противодействия неправомерному завладению компьютерной информацией» проводится сравнительно-правовой анализ уголовного законодательства ряда стран Западной Европы, государств-участников СНГ и иных государств в части ответственности за неправомерное завладение компьютерной информацией. Констатируется, что уголовные законы государств содержат специальные нормы об ответственности за неправомерное завладение компьютерной информацией, однако унифицированные подходы к криминализации и описанию указанных деяний в законе отсутствуют. Отмечается, что в ряде государств завладение компьютерной информацией является преступлением только при условии, если ему предшествовал несанкционированный доступ, а в большинстве государств – относится к делам частно-публичного обвинения, то есть к делам, которые возбуждаются только по заявлению пострадавшего лица.

Анализ уголовного законодательства государств-участников СНГ показал, что все государства Содружества включили в принятые уголовные кодексы самостоятельные главы, предусматривающие уголовную ответственность за преступления, посягающие на информационную

безопасность. В зависимости от круга деяний, признаваемых преступлениями, и его соотношения с модельным УК для государств-участников СНГ выделены две модели установления уголовной ответственности за указанные преступления в их уголовных кодексах: 1) основанная на модельном УК («расширенная») и 2) «российская» модель («усеченная»). В последующем автором выделены два основных подхода к криминализации неправомерного завладения компьютерной информацией в уголовных законах государств-участников СНГ: прямой уголовно-правовой запрет и придание неправомерному (несанкционированному) копированию компьютерной информации статуса одного из последствий несанкционированного доступа к компьютерной информации. Отмечается несовершенство каждого из выделенных подходов, в связи с чем указывается на целесообразность выработки оптимального подхода (модели) к криминализации неправомерного завладения компьютерной информации не только в рамках главы о преступлениях против информационной безопасности, но и в целом системы уголовного закона. В этой связи автором предложена модель уголовно-правовой регламентации деяний, связанных с противоправным получением компьютерной информации, которая направлена на обеспечение системности уголовного закона и исключение проблемных вопросов юридической оценки таких деяний.

Вторая глава ***«Уголовно-правовая характеристика состава неправомерного завладения компьютерной информацией»*** включает четыре раздела. *Первый раздел* посвящен вопросам определения родового и непосредственного объектов неправомерного завладения компьютерной информацией. Сквозь призму нормативного определения раскрывается содержание понятия «информационная безопасность». Анализ положений уголовного закона и иных правовых актов свидетельствует о довольно широкой трактовке данного понятия, которое недостаточно точно отражает родовой объект преступлений, предусмотренных гл. 31 УК. Под родовым объектом неправомерного завладения компьютерной информацией предложено понимать общественные отношения по обеспечению безопасности компьютерной информации, то есть общественные отношения, обеспечивающие состояние защищенности (конфиденциальности, целостности, подлинности, доступности и сохранности) компьютерной информации при ее получении, передаче, обработке, накоплении, хранении, распространении, предоставлении, а также компьютеров, компьютерных систем и сетей, машинных носителей, содержащих, обрабатывающих или передающих такую информацию.

Обосновано, что неправомерное завладение компьютерной информацией является многообъектным преступлением, раскрыто содержание основного

и дополнительного непосредственного объекта. Одновременно подчеркивается, что несанкционированное копирование посягает более на конфиденциальность компьютерной информации, в то время как иное неправомерное завладение, связанное с изъятием информации у обладателя, – на сохранность и доступность такой информации.

В разделе 2.2 «Предмет неправомерного завладения компьютерной информацией» анализируются научные подходы к уголовно-правовому определению терминов «информация», «компьютерная информация». Констатируется, что общепризнанное, универсальное доктринальное и законодательное определение компьютерной информации отсутствует. В связи со сложностью и многообразием форм и состояний информации, неотделимостью ее от носителя отмечается, что без привязки к материальному носителю определение термина «компьютерная информация» вызывает неоднозначное понимание и трудности правоприменения. На основе выделенных признаков, которыми должна обладать информация для отнесения ее к предмету преступления, предусмотренного ст. 352 УК, сформулировано определение компьютерной информации, которое предлагается закрепить в примечании к гл. 31 УК. Одновременно раскрывается содержание понятий «машинный носитель» и «компьютер». При рассмотрении вопроса о влиянии установленного законодательством правового режима информации на отнесение ее к предмету неправомерного завладения компьютерной информацией обосновывается, что предметом данного преступления может выступать не только информация ограниченного распространения, но и общедоступная информация.

В разделе 2.3 «Объективная сторона неправомерного завладения компьютерной информацией» с учетом результатов научных исследований и судебно-следственной практики анализируются признаки объективной стороны рассматриваемого состава преступления – деяние, общественно опасные последствия и причинная связь между ними. Автором раскрываются такие признаки состава преступления, как «несанкционированное копирование», «перехват компьютерной информации», «иное неправомерное завладение». Автором определены признаки несанкционированного копирования компьютерной информации и иного неправомерного завладения, которые обусловливают необходимость дифференциации уголовной ответственности за их совершение. Также сделан вывод об отсутствии необходимости выделения в ст. 352 УК в качестве отдельного способа совершения преступления перехвата компьютерной информации, предложено исключить из статьи несанкционированное копирование компьютерной информации как один из способов неправомерного завладения.

Также в разделе рассматриваются проблемные аспекты определения существенного вреда в составе неправомерного завладения компьютерной информацией и причинной связи между деянием и общественно опасными последствиями. Ввиду отсутствия в доктрине и практике единых подходов к определению существенного вреда автором сформулирован примерный перечень последствий неправомерного завладения компьютерной информацией, признаваемых существенными, при их нематериальном характере, а также предложено закрепить в уголовном законе количественную характеристику существенного вреда в случае причинения имущественного вреда.

В *четвертом разделе* рассматриваются субъективные признаки состава неправомерного завладения компьютерной информации – субъективная сторона и субъект преступления. Констатируется, что конструкция ст. 352 УК допускает различное толкование нормы в части определения формы вины по отношению к общественно опасным последствиям в виде существенного вреда, анализируются позиции ученых по данному вопросу. По мнению автора, закрепление в статье, предусматривающей ответственность за неправомерное завладение компьютерной информацией, формы вины по отношению к последствиям, положительно отразится на правоприменении. Также в разделе рассматривается возможность дополнения состава квалифицирующими признаками, характеризующими субъективную сторону и субъект преступления, а также целесообразность понижения возраста уголовной ответственности за совершение преступлений против информационной безопасности. Сделан вывод об отсутствии такой необходимости.

Третья глава ***«Состав неправомерного завладения компьютерной информацией в системе Уголовного кодекса Республики Беларусь»*** включает два раздела. В *разделе 3.1 «Отграничение неправомерного завладения компьютерной информацией от иных преступлений против информационной безопасности»* рассмотрены вопросы отграничения неправомерного завладения компьютерной информацией от иных преступлений, предусмотренных гл. 31 УК, выделены основные разграничительные признаки. Отмечено, что на практике неправомерное завладение компьютерной информацией и несанкционированный доступ часто взаимосвязаны между собой и являются результатом реализации единого умысла виновного. Кроме того, имеется сходство непосредственного объекта двух преступлений, а также результата данных противоправных деяний. Сделан вывод о достаточности защиты отношений, обеспечивающих конфиденциальность компьютерной информации, посредством установления уголовной ответственности за несанкционированный доступ к компьютерной информации. Далее акцентировано внимание

на наличие проблем при разграничении компьютерного саботажа, модификации компьютерной информации и ее завладения, связанного с изъятием. Обоснована необходимость изложения ст. 350–352 УК в новой редакции.

В разделе 3.2 «Неправомерное завладение компьютерной информацией как один из признаков преступлений, в которых компьютерная информация выступает предметом или средством совершения преступления» рассмотрены вопросы квалификации неправомерного завладения компьютерной информацией. Особое внимание уделено особенностям юридической оценки неправомерного завладения компьютерной информацией при последующем совершении преступлений против собственности. В частности, рассматривается возможность отнесения компьютерной информации к предмету хищения, соотношение неправомерного завладения с преступлениями, предусмотренными ст. 212 и 216 УК. Обосновано, что действия по несанкционированному копированию реквизитов банковских платежных карт не входят в объективную сторону совершаемого с их использованием хищения и должны получать самостоятельную уголовно-правовую оценку. Также рассмотрены вопросы соотношения исследуемого состава с составами преступлений, предусмотренными ст. 179, 254 УК и др. В завершении автором сформулированы рекомендации по квалификации деяний, сопряженных с противоправным получением компьютерной информации.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

Проведенное исследование позволяет сформулировать следующие положения теоретического и прикладного характера:

1. Комплексное рассмотрение национального законодательства, научных работ в области уголовного и информационного права позволяет сделать вывод, что правовой режим той или иной информации обусловливается характером сведений, которые содержит информация, и возможностью наступления негативных последствий ее свободного оборота, а не объективной формой ее представления. На основе указанных принципов выстраивалась система «информационных» преступлений в ранее действовавшем УК 1960 г., УК 1999 г. В этой связи с целью обеспечения системности уголовного закона и исключения проблемных вопросов юридической оценки общественно опасных деяний, связанных с противоправным получением (собиранием, похищением, копированием, завладением, перехватом) компьютерной информации, предложена авторская модель уголовно-правовой регламентации таких деяний, основанная на совокупности следующих положений:

1) при установлении уголовной ответственности за деяния, связанные с противоправным получением информации, в том числе компьютерной, основными критериями криминализации должны выступать содержание информации, являющейся предметом преступления (различные виды охраняемых законом тайн), и, соответственно, установленный в отношении информации правовой режим. Общественная опасность таких деяний обусловливается причинением (возможностью причинения) существенного вреда в результате неправомерного обладания данной информацией, включая последующее ее использование (разглашение), и не может определяться только формой представления информации;

2) установление в гл. 31 УК уголовной ответственности только за такие способы противоправного получения компьютерной информации, которые сопряжены с причинением существенного вреда исходя из компьютерной формы представления информации, являющейся предметом преступления [7; 10; 16; 26].

2. С учетом наличия в уголовном законе составов преступлений, предусматривающих ответственность за различные формы противоправного получения информации исходя из ее содержания, а также содержания родового объекта состава неправомерного завладения компьютерной информацией, к которому отнесены общественные отношения по обеспечению безопасности компьютерной информации, и предмета данного преступления, в качестве которого может выступать общедоступная информация и информация, распространение и (или) предоставление которой ограничено, определено основание установления в ст. 352 УК самостоятельной уголовной ответственности за данное деяние. Таковым является общественная опасность деяния, выражающаяся в его свойстве причинить существенный вред охраняемым уголовным законом отношениям независимо от установленного в отношении компьютерной информации, являющейся предметом преступления, правового режима (банковская или коммерческая тайна, тайна личной жизни и др.). Предложенное определение основания криминализации неправомерного завладения компьютерной информацией раскрывает сущность уголовно-правового запрета, изложенного в ст. 352 УК, а также позволяет обозначить направления совершенствования норм об ответственности за его совершение и практики их применения [1; 3; 7; 8; 13; 15; 20; 25; 26].

3. На основе сравнительного анализа уголовного законодательства государств-участников СНГ выделены две модели установления уголовной ответственности за компьютерные преступления в уголовных кодексах («расширенная» и «российская» модель) и два основных подхода к криминализации неправомерного копирования компьютерной информации

(прямой уголовно-правовой запрет и придание неправомерному (несанкционированному) копированию компьютерной информации статуса одного из последствий несанкционированного доступа к компьютерной информации). Установлена совокупность признаков несанкционированного копирования компьютерной информации, которая обусловливает особенности уголовно-правовой регламентации ответственности за совершение данного деяния в сравнении с существующими в национальном уголовном законодательстве и уголовном законодательстве государств-участников СНГ подходами к его криминализации. Определено, что непосредственным объектом несанкционированного копирования компьютерной информации в отличие от иного неправомерного завладения компьютерной информацией выступают общественные отношения по обеспечению конфиденциальности (неизвестности) информации, а общественную опасность данного деяния альтернативно обусловливают следующие факторы: установленный законодательством в отношении информации правовой режим (например, отнесение информации к государственным секретам, банковской, коммерческой тайне); цель, преследуемая виновным при копировании компьютерной информации (например, последующее совершение преступления с использованием информации); субъективная оценка характера и степени причиненного обладателю информации вреда в зависимости от важности (ценности) для него информации [2; 8; 9; 20; 24; 25].

4. С целью совершенствования правового регулирования уголовной ответственности за неправомерное завладение компьютерной информацией сформулированы и обоснованы следующие предложения по корректировке уголовного закона:

4.1 дифференциация уголовной ответственности за перечисленные в ст. 352 УК деяния (несанкционированное копирование, иное неправомерное завладение) путем исключения из статьи несанкционированного копирования компьютерной информации как одного из способов неправомерного завладения компьютерной информацией. Обосновывается целесообразность сохранения в ст. 352 УК ответственности только за завладение компьютерной информацией, под которым предлагается понимать умышленные действия виновного лица по получению компьютерной информации, в том числе путем перехвата, в результате которых обладатель информации либо ее получатель лишаются возможности использовать данную информацию, то есть действия и их результат, связанные с изъятием информации у обладателя. Реализация данного предложения не повлечет возникновение пробела в правовом регулировании [3; 6–10; 18; 20; 27];

4.2 целостность, доступность и сохранность информации в равной мере определяют ее значимость для обладателя. Фактические последствия завладения компьютерной информацией для обладателя равнозначны уничтожению и блокированию информации и выражаются в невозможности ее использования и утрате. В этой связи обосновывается целесообразность унификации законодательной конструкции уголовно-правовых норм гл. 31 УК, предусматривающих ответственность за компьютерный саботаж, модификацию компьютерной информации и неправомерное завладение компьютерной информацией. Ввиду однородности характера противоправного поведения, близкой степени общественной опасности, отсутствия четких разграничительных признаков между завладением, уничтожением, блокированием, модификацией компьютерной информации предлагается рассматривать их как равнозначные способы посягательства на безопасность компьютерной информации. В этой связи аргументируется изложение ст. 350–352 УК в новой редакции, предусматривающей их сходную структуру (материальная конструкция состава, идентичные квалифицирующие признаки), равный диапазон видов и размера наказаний [6; 9; 10; 20; 28];

4.3 установление повышенной ответственности за противоправное получение компьютерной информации путем дополнения составов преступлений, предусматривающих ответственность за противоправное получение сведений безотносительно формы их представления, таким квалифицирующим признаком, как «сопряженность с несанкционированным доступом к компьютерной информации, компьютерной системе или сети». Данный квалифицирующий признак одновременно указывает на особенности предмета преступления (компьютерную информацию) и отражает значительное увеличение степени общественной опасности запрещаемого деяния в сравнении с деянием, предусмотренным основным составом [5; 7; 8; 10].

Перечисленные и иные предложения по совершенствованию уголовно-правовой регламентации ответственности за неправомерное завладение компьютерной информацией оформлены в виде законопроекта, предусматривающего внесение следующих дополнений и изменений в уголовный закон:

– дополнение ч. 2 ст. 179 и ч. 2 ст. 254 УК после слов «информации» и «размере» соответственно словами «либо сопряженные (-ый) с несанкционированным доступом к компьютерной информации, компьютерной системе или сети»;

– дополнение гл. 31 УК примечаниями, в которых изложена дефиниция компьютерной информации, а также на основе дифференцированного подхода

определен размер имущественного вреда, признаваемого существенным, – ущерб в значительном размере;

– в ст. 352 УК предлагается:

слова «существенного вреда» заменить словами «ущерба в значительном размере либо иного существенного вреда»;

за действия, предусмотренные основным составом, в качестве максимального вида и размера наказания установить лишение свободы на срок до трех лет;

дополнить статью квалифицирующим признаком, предусмотренным ч. 3 ст. 349 УК;

дополнить статью примечанием, раскрывающим содержание понятия «завладение компьютерной информацией»;

– изложение ст. 350–351 УК в новой редакции, а также дополнение Кодекса ст. 352-1 УК, предусматривающей ответственность за принуждение к передаче компьютерной информации [1; 3; 6; 8–10; 13; 18–20; 23; 26].

5. На основе анализа проблемных вопросов, возникающих в судебно-следственной практике, сформулированы рекомендации по квалификации деяний, связанных с противоправным получением компьютерной информации. Так, при юридической оценке указанных деяний предлагается руководствоваться следующими правилами:

признание неправомерного завладения компьютерной информацией в качестве преступления, предусмотренного ст. 352 УК, не должно ставиться в зависимость от последующего использования (неиспользования) данной информации в преступных целях;

действия, выражающиеся в противоправном получении компьютерной информации с целью совершения конкретного преступления (менее тяжкого, тяжкого или особо тяжкого), наряду с приготовлением к его совершению должны получать самостоятельную уголовно-правовую оценку по соответствующим статьям уголовного закона, предусматривающим ответственность за противоправное получение информации;

если неправомерное завладение компьютерной информацией выступает в качестве способа совершения иного преступления, имеет место совокупность преступления, предусмотренного ст. 352 УК, и соответствующего преступления, способом которого явилось неправомерное завладение компьютерной информацией [4; 6; 9; 17; 21; 26].

Рекомендации по практическому использованию результатов

Результаты исследования могут быть использованы государственными органами при разработке проектов нормативных правовых актов, направленных на совершенствование уголовного законодательства в данной сфере (справка

Постоянной комиссии Палаты представителей Национального собрания Республики Беларусь по законодательству), при подготовке и проведении обобщения судебной практики применения положений гл. 31 УК (письмо Верховного Суда Республики Беларусь), а также внедрены в практическую деятельность Государственного секретариата Совета Безопасности Республики Беларусь, подразделений Следственного комитета Республики Беларусь и Российской Федерации, Генеральной прокуратуры Республики Беларусь (акт Государственного секретариата Совета Безопасности Республики Беларусь, акт Следственного комитета Республики Беларусь, акт Главного управления криминалистики Следственного комитета Российской Федерации, акт Генеральной прокуратуры Республики Беларусь), в учебный процесс учреждений образования, в том числе при реализации программ повышения квалификации сотрудников правоохранительных органов (акт Белорусского государственного университета, акт УО «Институт национальной безопасности Республики Беларусь», акт УО «Академия Министерства внутренних дел Республики Беларусь», акт УО «Институт переподготовки и повышения квалификации судей, работников прокуратуры, судов и учреждений юстиции Белорусского государственного университета», акт УО «Полоцкий государственный университет»).

Выводы и научные положения, сформулированные в диссертации, могут служить материалом для последующих исследований в области уголовно-правовой борьбы с преступлениями против информационной безопасности.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в журналах и сборниках, включенных в Перечень научных изданий Республики Беларусь для опубликования результатов диссертационных исследований

1. Дубко, М. А. Объективные признаки неправомерного завладения компьютерной информацией / М. А. Дубко // Вестн. Полоц. гос. ун-та. Сер. D, Экон. и юрид. науки. – 2012. – № 13. – С. 180–184.

2. Дубко, М. А. Международное сотрудничество в сфере уголовно-правовой борьбы с неправомерным завладением компьютерной информацией / М. А. Дубко // Вестн. Полоц. гос. ун-та. Сер. D, Экон. и юрид. науки. – 2012. – № 14. – С. 180–183.

3. Дубко, М. А. Проблемные аспекты определения конструктивных признаков неправомерного завладения компьютерной информацией /

М. А. Дубко // Проблемы укрепления законности и правопорядка: наука, практика, тенденции : сб. науч. тр. / Науч.-практ. центр проблем укрепления законности и правопорядка Генер. прокуратуры Респ. Беларусь ; редкол.: В. М. Хомич [и др.]. – Минск : РИПО, 2015. – Вып. 8. – С. 76–82.

4. Дубко, М. А. Особенности квалификации неправомерного завладения компьютерной информацией и отграничения от иных преступлений против информационной безопасности / М. А. Дубко // Вестн. Полоц. гос. ун-та. Сер. D, Экон. и юрид. науки. – 2015. – № 13. – С. 180–186.

5. Дубко, М. А. Субъективные признаки неправомерного завладения компьютерной информацией / М. А. Дубко // Вестн. Полоц. гос. ун-та. Сер. D, Экон. и юрид. науки. – 2015. – № 14. – С. 188–192.

6. Дубко, М. А. Неправомерное завладение компьютерной информацией: существенный вред в составе преступления / М. А. Дубко // Право.by. – 2016. – № 3. – С. 39–45.

7. Дубко, М. А. Основание и причины криминализации неправомерного завладения компьютерной информацией / М. А. Дубко // Вестн. Акад. МВД Респ. Беларусь. – 2017. – № 1 (33). – С. 87–91.

8. Дубко, М. А. Несанкционированное копирование как способ неправомерного завладения компьютерной информацией / М. А. Дубко // Законность и правопорядок. – 2017. – № 4. – С. 58–63.

9. Дубко, М. А. Отдельные вопросы уголовно-правовой защиты компьютерной информации от неправомерного завладения / М. А. Дубко // Проблемы укрепления законности и правопорядка: наука, практика, тенденции : сб. науч. тр. / Науч.-практ. центр проблем укрепления законности и правопорядка Генер. прокуратуры Респ. Беларусь ; редкол.: В. В. Марчук [и др.]. – Минск : Изд. центр БГУ, 2017. – Вып. 10. – С. 90–96.

10. Дубко, М. А. Совершенствование уголовно-правовой регламентации ответственности за неправомерное завладение компьютерной информации (ст. 352 УК) / М. А. Дубко // Вестн. Акад. МВД Респ. Беларусь. – 2018. – № 1 (35). – С. 133–137.

Материалы конференций

11. Дубко, М. А. Уголовно-правовая защита компьютерной информации в законодательстве зарубежных стран / М. А. Дубко // Интеграционные экономико-правовые направления развития Украины и стран ближнего зарубежья : сб. ст. междунар. конф., Львов, 31 янв. 2012 г. [Электронный ресурс]. – Режим доступа: http://lac.lviv.ua. – Дата доступа: 20.02.2012.

12. Dubko, M. Unauthorized capture of computer information in foreign and international law / M. Dubko // Nationl and European context in research : materials

of junior researcher’s III conference : In 3 Parts, Novopolotsk, April 25–26, 2012. – Novopolotsk : Polotsk State University, 2012. – Part 1. – С. 51–53.

13. Дубко, М. А. Особенности предмета неправомерного завладения компьютерной информацией / М. А. Дубко // Современные тенденции развития юридической науки, правового образования и воспитания : материалы междунар. науч.-практ. конф. : в 2 т., Полоцк, 18–19 мая 2012 г. / редкол.: А. Н. Пугачев (отв. ред.) [и др.]. – Новополоцк : ПГУ, 2012. – Т. 2. – С. 114–118.

14. Дубко, М. А. Электронный документ как предмет неправомерного завладения компьютерной информацией / М. А. Дубко // Научные стремления – 2012 : сб. материалов III Междунар. молодеж. науч.-практ. конф. : в 2 т., Минск, 6–9 нояб. 2012 г. / Совет молодых ученых Нац. акад. наук Беларуси. – Минск : Белорусская наука, 2012. – Т. 2 – С. 74–77.

15. Дубко, М. А. Проблемы определения родового и непосредственного объекта неправомерного завладения компьютерной информации / М. А. Дубко // Вклад молодых ученых в развитие правовой науки Республики Беларусь : сб. материалов III Междунар. науч. конф., Минск, 23 нояб. 2012 г. / Национал. центр законодательства и правовых исследований Респ. Беларусь ; редкол.: В. И. Семенков (гл. ред) [и др.]. – Минск : Бизнесофсет, 2012. – С. 301–304.

16. Дубко, М. А. Деятельность государств-участников СНГ в сфере уголовно-правовой борьбы с неправомерным завладением компьютерной информацией / М. А. Дубко // Преступления в информационной сфере: проблемы расследования, квалификации, реализации ответственности и предупреждения : материалы Междунар. науч. конф., Тамбов, 14–15 фев. 2013 г. / М-во обр. и науки РФ, ФГБОУ ВПО «Тамб. гос. ун-т им. Г.Р. Державина» ; редкол.: В. А. Шуняева, Е. А. Попова, С. А. Пучнина. – Тамбов : Изд. дом ТГУ им. Г. Р. Державина, 2013. – С. 228–233.

17. Дубко, М. А. Отграничение неправомерного завладения компьютерной информацией от смежных составов по уголовному закону Республики Беларусь / М. А. Дубко // Людина, суспільство, держава: правовий вимір в сучасному світі : материалы IV междунар. науч.-практ. конф., Киев, 27 февр. 2014 г. [Электронный ресурс]. – Режим доступа: http://conference.nau.edu.ua/index.php/ TL/PRAVVYMIR/paper/view/1477/858. – Дата доступа: 17.03.2014.

18. Дубко, М. А. Оптимизация уголовной ответственности за неправомерное завладение компьютерной информацией / М. А. Дубко // Теоретические и прикладные аспекты современной юридической науки : сб. материалов Междунар. науч.-практ. конф., посвященной памяти проф. В. И. Семенкова, Минск, 11 дек. 2015 г. / Национал. центр законодательства

и правовых исследований Респ. Беларусь; редкол.: С. М. Сивец [и др.]. – Минск : Институт радиологии, 2015. – С. 299–301.

19. Дубко, М. А. Неправомерное завладение компьютерной информацией: существенный вред в составе преступления / М. А. Дубко // Борьба с преступностью: теория и практика [Электронный ресурс] : тезисы докладов IV Междунар. науч.-практ. конф., Могилев, 25 марта 2016 г. / М-во внутр. дел Респ. Беларусь, Могилев. ин-т М-ва внутр. дел Респ. Беларусь ; редкол.: Ю. П. Шкаплеров (отв. ред.) [и др.]. – Могилев : Могилев. ин-т МВД, 2016. – 1 электрон. опт. диск (CD-R).

20. Дубко, М. А. Несанкционированное копирование в составе неправомерного завладения компьютерной информацией / М. А. Дубко // Проблемы борьбы с преступностью и подготовки кадров для правоохранительных органов : тезисы докладов междунар. науч.-практ. конф., посвященной 100-летию милиции Беларуси, Минск, 10 февр. 2017 г. / Акад. М-ва внутр. дел Респ. Беларусь ; редкол.: А. В. Яскевич (отв. ред) [и др.]. – Минск : Акад. М-ва внутр. дел Респ. Беларусь, 2017. – С. 154–155.

21. Дубко, М. А. Уголовно-правовая оценка действий, сопряженных с противоправным завладением реквизитами банковских платежных карт / М. А. Дубко // Традиции и инновации в праве : материалы междунар. науч.-практ. конф., посвящ. 20-летию юрид. фак. и 50-летию Полоц. гос. ун-та, Новополоцк, 6–7 окт. 2017 г. : в 3 т. / Полоцкий гос. ун-т, Регион. учеб.-науч.-практ. Юрид. центр ; редкол.: И. В. Вегера (отв. ред.) [и др.]. – Новополоцк : Полоц. гос. ун-т, 2017. – Т. 3. – С. 32–35.

Статьи в сборниках научных трудов, информационно-практических изданиях, электронных правовых системах и ресурсах

22. Дубко, М. А. Развитие теоретических исследований в области информации, информатизации и борьбы с компьютерными преступлениями / М. А. Дубко // Центр исследования компьютерной преступности. Статьи. [Электронный ресурс]. – Режим доступа: http://www.crime-research.ru/articles/7653/. – Дата доступа: 02.10.2013.

23. Дубко, М. А. Существенный вред как обязательный признак неправомерного завладения компьютерной информацией / М. А. Дубко // Правотворчество и правоприменение в условиях инновационного общества : сб. науч. ст. : в 2 ч. / редкол.: Н. В. Сильченко (гл. ред.) [и др.]. – Гродно : ГрГМУ, 2014. – Ч. 2. – С. 289–294.

24. Дубко, М. А. Уголовное законодательство государств-участников Содружества Независимых Государств, предусматривающее ответственность

за неправомерное завладение компьютерной информацией: сравнительно-правовой анализ (по сост. на 05.01.2015) [Электронный ресурс] / М. А. Дубко // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр». – Минск, 2018.

25. Дубко, М. А. Понятие компьютерного преступления (по сост. на 10.08.2015) [Электронный ресурс] / М. А. Дубко // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр». – Минск, 2018.

26. Дубко, М. А. Компьютерная информация как предмет преступления, предусмотренного ст. 352 Уголовного кодекса Республики Беларусь (по сост. на 15.02.2016) [Электронный ресурс] / М. А. Дубко // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр». – Минск, 2018.

27. Дубко, М. А. Подходы к определению существенного вреда в составе неправомерного завладения компьютерной информацией (ст. 352 Уголовного кодекса Республики Беларусь) (по сост. на 29.09.2016) [Электронный ресурс] / М. А. Дубко // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр». – Минск, 2018.

28. Дубко, М. А. Отдельные вопросы уголовной ответственности за преступления против информационной безопасности в Республике Беларусь / М. А. Дубко // Вестн. Глав. управ. криминалистики Следств. ком. Рос. Федерации. – 2017. – № 11 (20). – С. 6–13.

РЭЗЮМЭ

Дубко Міхаіл Анатольевіч

Неправамернае завалоданне камп'ютэрнай інфармацыяй як злачынства супраць інфармацыйнай бяспекі

Ключавыя словы: інфармацыйная бяспека, неправамернае завалоданне камп'ютэрнай інфармацыяй, несанкцыяніраванае капіраванне, камп'ютэрная інфармацыя.

Мэта даследавання: распрацоўка тэарэтычных палажэнняў крымінальнай адказнасці за неправамернае завалоданне камп'ютэрнай інфармацыяй і выраб прапаноў па ўдасканальванні крымінальнага закона і практыкі яго прымянення ў дадзенай частцы.

Метады даследавання: агульнанавуковыя і спецыяльныя метады пазнання: аналіз, сінтэз, параўнальна-прававы, фармальна-лагічны, сацыялагічны, метад статыстычнага і сістэмна-структурнага аналізу.

Атрыманыя вынікі і іх навізна: прадстаўленая дысертацыя з'яўляецца першай у Рэспубліцы Беларусь работай, у якой праведзена даследаванне пытанняў крымінальна-прававой рэгламентацыі адказнасці за неправамернае завалоданне камп'ютэрнай інфармацыяй. У выніку вызначана падстава крыміналізацыі неправамернага завалодання камп'ютэрнай інфармацыяй і адметныя адзнакі несанкцыяніраванага капіравання камп'ютэрнай інфармацыі, якія абумоўліваюць асаблівасці крымінальна-прававой рэгламентацыі адказнасці за ўчыненне дадзенага дзеяння, сфармуляваны і абгрунтаваны канкрэтныя прапановы па карэкціроўцы крымінальна-прававых норм гл. 31 крымінальнага закона, а таксама правапрымяняльнай практыкі, распрацаваны рэкамендацыі па кваліфікацыі дзеянняў, звязаных з проціпраўным атрыманнем (збіраннем, крадзяжом, капіраваннем, завалоданнем, перахватам) камп'ютэрнай інфармацыі. У рамках даследавання ўпершыню распрацавана мадэль крымінальна-прававой рэгламентацыі такіх дзеянняў.

Рэкамендацыі па выкарыстанні: вынікі даследавання ўкаранёны ў праваахоўную дзейнасць, адукацыйны працэс ўстаноў адукацыі Рэспублікі Беларусь.

Вобласць прымянення: навуковая, заканатворчая, практычная дзейнасць і адукацыйны працэс.

РЕЗЮМЕ

Дубко Михаил Анатольевич

Неправомерное завладение компьютерной информацией как преступление против информационной безопасности

Ключевые слова: информационная безопасность, неправомерное завладение компьютерной информацией, несанкционированное копирование, компьютерная информация.

Цель исследования: разработка теоретических положений уголовной ответственности за неправомерное завладение компьютерной информацией и выработка предложений по совершенствованию уголовного закона и практики его применения в данной части.

Методы исследования: общенаучные и специальные методы познания: анализ, синтез, сравнительно-правовой, формально-логический, социологический, метод статистического и системно-структурного анализа.

Полученные результаты и их новизна: представленная диссертация является первой в Республике Беларусь работой, в которой проведено исследование вопросов уголовно-правовой регламентации ответственности за неправомерное завладение компьютерной информацией. В результате определены основание самостоятельной криминализации неправомерного завладения компьютерной информацией и признаки несанкционированного копирования компьютерной информации, которые обусловливают особенности уголовно-правовой регламентации ответственности за совершение данного деяния, сформулированы и обоснованы конкретные предложения по корректировке уголовно-правовых норм, содержащихся в гл. 31 УК, а также практики их применения, разработаны рекомендации по квалификации деяний, связанных с противоправным получением (собиранием, похищением, копированием, завладением, перехватом) компьютерной информации. В рамках исследования впервые разработана модель уголовно-правовой регламентации таких деяний.

Рекомендации по использованию: результаты исследования внедрены в правоохранительную деятельность, образовательный процесс ряда учреждений образования Республики Беларусь.

Область применения: научная, законотворческая, правоприменительная практика и образовательный процесс.

SUMMARY

Mikhail A. Dubko

Illegal acquisition of computer information as a crime against information security

Keywords: information security, illegal possession of computer information, unauthorized copying, computer information.

Aim of the research work: a comprehensive analysis of the problems of application of art. 352 of the Criminal Code and the development on this basis of proposals to improve the criminal law and practice of its application in terms of criminal liability for the unlawful acquisition of computer information.

Research methods: general scientific and special methods of cognition: analysis, synthesis, comparative legal, formal logical, sociological, method of statistical and system-structural analysis.

Results and their novelty: the presented thesis is the first in the Republic of Belarus work in which a comprehensive study of the issues of criminal responsibility for the misuse of computer information. As a result, the basis for criminalization of the unlawful acquisition of computer information has been determined, specific suggestions have been formulated and substantiated for correcting the criminal law contained in Ch. 31 of the Criminal Code, as well as the practice of law enforcement, developed recommendations for the qualification of acts involving the misuse of computer information. The research for the first time developed a theoretical approach to the establishment of criminal liability for socially dangerous acts related to unlawful receipt (collection, abduction, copying, seizure, etc.) of information.

Recommendations on the use: the results of the research are introduced into law enforcement activities, the educational process of a number of educational institutions of the Republic of Belarus.

Application area: scientific, legislative, law enforcement practice and educational process.