БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УДК 343.534(476)(043.3)

ПОЛЕЩУК
ДМИТРИЙ ГРИГОРЬЕВИЧ

УГОЛОВНО-ПРАВОВАЯ ОХРАНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (НА ПРИМЕРЕ ОТДЕЛЬНЫХ АСПЕКТОВ ОХРАНЫ КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ)

Автореферат
диссертации на соискание ученой степени
кандидата юридических наук

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

Минск, 2020

Научная работа выполнена в Национальном центре законодательства и правовых исследований Республики Беларусь

Научный руководитель	**Шаблинская Диана Викторовна,** кандидат юридических наук, доцент, заведующий сектором правового обеспечения экономической безопасности Центра государственного строительства и права ГНУ «Институт экономики Национальной академии наук Беларуси»
Официальные оппоненты:	**Савенок Анатолий Леонидович,** доктор юридических наук, профессор, заслуженный работник образования Республики Беларусь, заведующий кафедрой уголовного права Белорусского государственного университета
	Лосев Владимир Владимирович, кандидат юридических наук, доцент, ректор учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО»
Оппонирующая организация	**ГУО «Институт национальной безопасности Республики Беларусь»**

Защита состоится 24 ноября 2020 года в 14:00 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 «_____» октября 2020 года.

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

ВВЕДЕНИЕ

Вопросы обеспечения информационной безопасности в настоящее время становятся все более актуальными, о чем свидетельствует принятие Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1.

Информация и информационная технология все чаще выступают как предметом, так и средством совершения общественно опасных посягательств в информационной сфере. В свое время действенным прогрессивным ответом на появление новых форм противоправного поведения стало включение в Уголовный кодекс Республики Беларусь 1999 г. (далее – УК) раздела XII «Преступления против информационной безопасности» и одноименной гл. 31. Тем не менее за истекший период внедрены новые информационные технологии (Wi-fi, блокчейн и др.), глобальная компьютерная сеть Интернет стала использоваться в качестве основного источника получения информации, обновилось регулятивное законодательство, что обусловило отдельные практические проблемы и создало предпосылки совершенствования уголовного закона. В такой ситуации уголовно-правовая охрана информационной безопасности призвана отражать статику и динамику информационной сферы, предупреждать негативные последствия для личности, общества и государства.

Эффективное противодействие преступлениям против информационной безопасности требует постоянного совершенствования нормативной правовой базы с учетом реально существующих общественных отношений, гармонизации уголовно-правовых норм и международного сотрудничества между государствами. Например, становление уголовно-правовой охраны информации о частной жизни и персональных данных как вида информации ограниченного распространения, оказывающего непосредственное влияние на информационную безопасность личности, стало возможным во второй половине XX в. в условиях укрепления права на неприкосновенность частной жизни и осознания важности защиты информации персонифицированного характера, в том числе при использовании информационных технологий. В то же время отдельные положения УК имеют расхождения с нормами законодательства об информации, информатизации и защите информации, а некоторые деяния не нашли закрепления в уголовном законе и остаются не в полной мере изученными (распространение вредоносных компьютерных программ, кибератаки, незаконный оборот паролей (кодов) доступа, обработка персональных данных и др.).

В связи с этим тема диссертационного исследования имеет актуальный характер и с учетом современных потребностей развития государства нуждается в системном и комплексном научно-практическом изучении.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с научными программами (проектами), темами

Диссертационное исследование проведено в соответствии с Концепцией национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, Концепцией информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, и осуществлялось в рамках научно-исследовательской темы Национального центра законодательства и правовых исследований Республики Беларусь (далее – НЦЗПИ) «Формирование новой правоохранительной политики как основа эффективной стратегии противодействия правонарушениям и обеспечения стабильности социально-экономических преобразований» (шифр «История, культура, общество, государство 5.08») подпрограммы 5 «Право и управление» Государственной программы научных исследований на 2011–2015 гг. «История, культура, общество, государство» (номер государственной регистрации 20110452).

Область диссертационного исследования соответствует п. 13 приоритетных направлений научных исследований Республики Беларусь на 2016–2020 гг., утвержденных постановлением Совета Министров Республики Беларусь от 12 марта 2015 г. № 190, и п. 15, 23, 36, 52, 229, 233, 234, 244, 245, 269, 329, 463, 466, 468, 469 Перечня актуальных направлений диссертационных исследований в области права на 2012–2016 гг., утвержденного решением межведомственного совета по проблемам диссертационных исследований в области права при Министерстве юстиции Республики Беларусь от 5 сентября 2012 г.

Цель и задачи исследования

Целью исследования является разработка теоретико-правовых основ уголовно-правовой охраны информационной безопасности, а также предложений по совершенствованию уголовного закона и практики его применения в части ответственности за посягательства на общественные отношения по поводу обеспечения информационной безопасности, кибербезопасности и защиты информации ограниченного распространения.

Указанной целью определены постановка и решение следующих задач:

– выявить сущностно-содержательные аспекты информационной безопасности как родового объекта преступлений против информационной безопасности и на данной основе разработать определение понятия «преступление против информационной безопасности», установить особенности описания преступлений, связанных с информационными технологиями, в УК и доктрине уголовного права;

– определить понятие кибербезопасности как видового объекта преступлений, предусмотренных гл. 31 УК;

– исследовать роль и значение информации как признака состава преступления в зависимости от ее формы и содержания;

– дать уголовно-правовую характеристику незаконных действий с вредоносными компьютерными программами (ст. 354 УК), оценить общественную опасность и провести уголовно-правовой анализ новых угроз, посягающих на кибербезопасность, на предмет возможной криминализации («спам», кибератака (DDoS-атака), незаконный оборот паролей, кодов доступа и иных аналогичных данных), разграничить их с преступлением, предусмотренным ст. 354 УК;

– изучить с позиции уголовного права гуманитарную составляющую информационной безопасности (защита конфиденциальной информации о частной жизни и персональных данных), оказывающую влияние на кибербезопасность в цифровую эпоху;

– проанализировать судебную практику по гл. 31 УК (преступления против информационной безопасности) и ст. 179 УК и выработать предложения по совершенствованию положений уголовного закона, а также правила квалификации исследуемых деяний.

Объектом диссертационного исследования являются общественные отношения, возникающие по поводу охраны информационной безопасности, установления и реализации уголовной ответственности в сфере обеспечения информационной безопасности. Предметом исследования являются научные суждения, нормы национального и зарубежного законодательства по вопросам уголовно-правовой охраны информационной безопасности, международно-правовые акты в данной области, а также практика их применения.

Научная новизна

Впервые проведено комплексное теоретико-практическое исследование современных проблем уголовно-правовой охраны информационной безопасности, а также понятия преступления против информационной безопасности (на основе выделения статичного и динамичного аспектов), сформулировано авторское определение данного понятия. Изложены новые научно обоснованные выводы и конкретные предложения по совершенствованию законодательства и правоприменения в сфере уголовно-правовой охраны информационной безопасности в целом и в частности кибербезопасности (компьютерной (цифровой) безопасности), защиты информации ограниченного распространения как основных составляющих информационной безопасности, а также защиты общества от информации негативного содержания. Для целей совершенствования юридической техники и устранения неоднозначного толкования норм уголовного закона предложены определение компьютерной (цифровой) информации, новая редакция ст. 354 УК, введение специальной нормы об уголовной ответственности за незаконные действия с персональными данными при наличии общественно

опасных последствий; проведен анализ таких новых деяний, посягающих на кибербезопасность (компьютерную (цифровую) безопасность), как распространение «спама», кибератака (DDoS-атака), незаконный оборот паролей, кодов доступа и иных аналогичных данных; обоснована необходимость защиты от информации негативного содержания уголовно-правовыми средствами.

Положения, выносимые на защиту

1. В действующем УК преступления против информационной безопасности рассматриваются в узком смысле – только как преступления против кибербезопасности (компьютерной (цифровой) безопасности) (гл. 31 УК). Вместе с тем понимание преступления против информационной безопасности в современных условиях не должно основываться исключительно на использовании информационных технологий в преступных целях, поскольку кибербезопасность является не единственным элементом информационной безопасности.

В контексте решения задач уголовного закона понятие информационной безопасности рассматривается в двух аспектах: ***статичном*** (защита компьютерной (цифровой) информации и поддерживающей ее инфраструктуры (кибербезопасность как *технологическая составляющая информационной безопасности*), защита информации, распространение и (или) предоставление которой ограничено, особенно информации о частной жизни и персональных данных, – *гуманитарная составляющая информационной безопасности*) и ***динамичном*** (защита от негативного воздействия информации).

Под информационной безопасностью в качестве объекта уголовно-правовой охраны следует понимать состояние защищенности информации и поддерживающей ее инфраструктуры, а также законных интересов граждан, общества или отдельных его институтов, государства в информационной сфере от внешних и внутренних угроз, обеспечивающее ее формирование, функционирование и развитие во благо граждан, общества и государства.

На основании выделения статичного (предметного) и динамичного (содержательного) аспектов исследуемой категории под ***преступлением против информационной безопасности*** предлагается понимать общественно опасное противоправное виновное деяние, непосредственно посягающее на компьютерную (цифровую) информацию и поддерживающую ее инфраструктуру, правовой режим информации, распространение и (или) предоставление которой ограничено законодательными актами, а также сопряженное с распространением информации, обращение которой запрещено законодательными актами.

Данные положения будут способствовать разработке новых подходов к уголовно-правовой охране информационной безопасности и повышению ее эффективности, реализации предупредительной и охранительной функций уголовного права, формированию новых научных категорий. Определение понятия преступления против информационной безопасности позволяет

разграничить способы и направленность совершения таких преступлений, что создаст основу совершенствования уголовного закона и его юридической техники.

2. В целях обеспечения единого понимания родового объекта преступлений против информационной безопасности и реализации положений национальных программных документов представляется обоснованным определить видовым объектом преступлений, предусмотренных гл. 31 УК, общественные отношения в сфере обеспечения ***кибербезопасности*** (компьютерной (цифровой) безопасности) как состояния защищенности информации в цифровой форме и поддерживающей ее инфраструктуры от любых угроз при использовании информационных технологий.

В уголовном законе необходимо закрепить понятие *компьютерной (цифровой) информации* как информации, хранящейся в компьютерной (информационной) системе, сети или на машинных носителях либо передаваемой в пространстве с помощью любых программно-технических средств.

Данные положения будут способствовать признанию цифровой информации предметом преступления с учетом роли формы информации в современном обществе и построении цифрового государства, а также ее отнесения к системообразующим компонентам кибербезопасности как отдельного объекта уголовно-правовой охраны. Закрепление в уголовном законе понятия компьютерной (цифровой) информации позволит унифицировать терминологию, устранить теоретические и практические противоречия при применении как норм гл. 31 УК, так и иных норм уголовного закона, направленных на охрану информационной безопасности.

Независимо от формы представления информация может носить и динамичный характер, когда она является неотъемлемым элементом определенного действия и уже не предметом, а средством совершения преступления. В статике могут нарушаться интересы обладателя информации, в динамике – получателя. В контексте *динамичного аспекта преступления против информационной безопасности* (уголовно-правовая защита от информации) представляется обоснованной криминализация распространения отдельных видов информации негативного содержания (информации, побуждающей к причинению телесных повреждений, оправдывающей терроризм и отрицающей преступления нацизма), в том числе в глобальной компьютерной сети Интернет.

3. На основании выявленных проблем развития информационной сферы и ее уголовно-правовой охраны, зарубежного опыта правового регулирования и положений международных договоров в целях повышения эффективности борьбы с преступлениями против информационной безопасности и обеспечения внутреннего единства данной деятельности предлагаются следующие направления оптимизации уголовно-правовой охраны кибербезопасности:

3.1. установить в уголовном законе минимальное количество технических

терминов и обеспечить точность и однозначность при формулировании признаков составов преступлений против информационной безопасности;

3.2. формулировать «технически нейтральные» конструкции уголовно-правовых норм, при этом использование современных информационных технологий рассматривать в качестве признака основного состава преступления, а не устанавливать в качестве квалифицирующего признака преступления;

3.3. усовершенствовать уголовно-правовые средства защиты от вредоносных компьютерных программ, в связи с чем в ст. 354 УК предлагается: исключить разделение вредоносных компьютерных программ на виды; криминализировать распространение и (или) предоставление вредоносной компьютерной программы; исключить термин «носители с такими программами»; включить в понятие «разработка вредоносной компьютерной программы» такое действие, как внесение изменений в существующие программы; дополнить ст. 354 УК квалифицирующими признаками «группа лиц по предварительному сговору» и (или) «организованная группа», а также «угроза наступления тяжких последствий»;

3.4. считать кибератаку (DoS- и DDoS-атаку) самостоятельной формой общественно опасного деяния, связанного с созданием препятствий для получения доступа законных пользователей к компьютерной (информационной) системе и, как правило, сопровождающегося использованием и (или) распространением вредоносных компьютерных программ. Кибератаку следует рассматривать в двух аспектах: как преступление против кибербезопасности (вид компьютерного саботажа (ст. 351 УК) и как преступление террористической или экстремистской направленности. Составы преступлений против информационной безопасности, установленные в УК, не в полной мере отражают существующую специфику DDoS-атак, не устанавливают все юридически значимые признаки их совершения (нарушение работы компьютерной (информационной) системы, учет угрозы наступления тяжких последствий, в том числе возможность причинения вреда критически важным объектам информатизации (далее – КВОИ)), в связи с чем положения ст. 351 УК нуждаются в совершенствовании;

3.5. ввести уголовную ответственность за отдельные незаконные действия с паролями в Республике Беларусь, дополнив гл. 31 УК ст. 353[1] «Незаконные изготовление, приобретение либо сбыт паролей, кодов доступа или иных аналогичных данных»;

3.6. признать распространение «спама» деянием, не подпадающим под признаки иных преступлений против информационной безопасности по своему содержанию и направленности, не имеющим в настоящее время достаточных предпосылок для криминализации в связи с отсутствием существенного вреда, присущего преступлению, либо возможности его причинения.

Реализация указанных предложений позволит усилить защиту человека, общества и государства от негативного воздействия вредоносных компьютерных

программ и новых угроз, посягающих на технологическую составляющую информационной безопасности (кибератаки (DoS- и DDoS-атаки), незаконный оборот паролей, кодов доступа или иных аналогичных данных).

4. С учетом выделения *гуманитарной составляющей информационной безопасности*, предполагающей, что конфиденциальная информация может выступать предметом преступления, в целях усиления информационной безопасности личности предлагается установить уголовную ответственность за незаконные действия с информацией о частной жизни и персональными данными как самостоятельными категориями информации ограниченного распространения, если содеянным причинен вред правам, свободам и законным интересам потерпевшего. Незаконные действия в отношении информации о частной жизни и персональных данных при отсутствии общественно опасных последствий, а также нарушение прав субъектов персональных данных (на получение информации об обработке его персональных данных и др.), правил защиты персональных данных не обладают общественной опасностью, присущей преступлению.

5. Системный характер изучения информационной безопасности как объекта уголовно-правовой охраны позволяет сформулировать рекомендации по практическому применению исследуемых норм уголовного закона и квалификации соответствующих деяний:

– квалификация противоправного использования информационных технологий возможна при отсутствии прямого указания на них в тексте УК;

– совершение незаконных действий с информацией о частной жизни и персональными данными, отображенными в форме компьютерной (цифровой) информации, влечет ответственность по совокупности преступлений с соответствующими составами преступлений, предусмотренными гл. 31 УК. В случае если информация о частной жизни или персональные данные являются составной частью иной информации ограниченного распространения (например, государственных секретов, материалов уголовного дела и др.), деяние квалифицируется по статье УК, предусматривающей ответственность за посягательство на указанную категорию информации ограниченного распространения;

– разработка вредоносной компьютерной программы включает в себя разработку специальной вирусной программы и может быть признана оконченной при наличии следующих условий: 1) компьютерная программа зафиксирована на материальном носителе в форме, доступной для восприятия техническими средствами (устройствами); 2) в алгоритме компьютерной программы содержится вредоносный код;

– время окончания использования специальных вирусных программ связано с началом контролируемого преступником их применения в информационных системах, сетях, машинных носителях, устройствах для определенных целей;

– окончанием распространения носителей с вредоносными компьютерными программами является момент вовлечения их в гражданский оборот в виде отчуждения в любой форме, а моментом окончания распространения вредоносной компьютерной программы в глобальной или локальной компьютерной сети – время ее размещения на определенном информационном ресурсе, в информационной системе, на сервере или устройстве, ином машинном носителе посредством удаленного доступа;

– носителем с вредоносной компьютерной программой является материальный объект (жесткий диск, Flash-накопитель, смартфон и др.), используемый для хранения и отображения информации, в том числе в виде вредоносной компьютерной программы;

– в случае уничтожения, блокирования, модификации либо копирования компьютерной информации, нарушения работы компьютерного оборудования, компьютерной (информационной) системы или сети, а также заведомого наступления тяжких последствий распространение носителей с вредоносными компьютерными программами (диски, Flash-накопители, смартфоны и др.) должно квалифицироваться по ч. 1 ст. 354 УК (распространение, предоставление или использование вредоносной компьютерной программы) и статьям УК, предусматривающим наступление соответствующих последствий;

– в качестве тяжких последствий, кроме указанных в ч. 3 ст. 349 УК, применительно к преступлениям против информационной безопасности (кибербезопасности) можно считать также причинение вреда КВОИ или объектам, которые подлежат отнесению к ним в порядке, предусмотренном законодательством;

– квалификация кибератак в качестве акта терроризма (международного терроризма) или диверсии при наличии уголовно-правовых признаков является допустимой и соответствует положениям Концепции информационной безопасности.

Реализация изложенных предложений и рекомендаций позволит сформировать единую правоприменительную практику и будет способствовать эффективной борьбе с преступлениями против информационной безопасности.

Личный вклад соискателя ученой степени

Диссертационное исследование выполнено автором самостоятельно. Предложения и выводы, содержащиеся в диссертации, основаны на изучении законодательства Республики Беларусь и зарубежных государств, международных норм и стандартов, судебной практики и доктринальных положений, изложенных в работах отечественных и зарубежных авторов.

Апробация диссертации и информация об использовании ее результатов

Результаты диссертационного исследования обсуждались на заседаниях отдела исследований в области правоохранительной деятельности и осуществления правосудия Института правовых исследований НЦЗПИ и апробированы на международных и республиканских научно-практических конференциях, научных форумах, в том числе: «Молодежная инициатива в решении современных проблем юриспруденции» (Минск, 25–26 октября 2013 г.), «Право и государство: история, современность, перспективы развития» (Минск, 24–25 октября 2014 г.), «Проблемы правотворческой и правоприменительной практики в условиях развития информационного общества» (Гродно, 5–6 марта 2015 г.), «Научно-образовательное пространство стран СНГ: история, достижения, потенциал» (Санкт-Петербург, 25 декабря 2015 г.), «Теоретические и прикладные аспекты информационной безопасности» (Минск, 31 марта 2016 г.), «Вклад молодых ученых в развитие правовой науки Республики Беларусь» (Минск, 2 июня 2017 г.), «Информационная революция и вызовы новой эпохи – стимулы формирования современных подходов к информационной безопасности» (Минск, 29–30 ноября 2018 г.), «Конституция Республики Беларусь как ценностный выбор: 25 лет свершений и преобразований» (Минск, 4 марта 2019 г.).

Основные выводы и предложения диссертационного исследования использованы в правотворческой и правоприменительной деятельности, в образовательном процессе, отражены в научном отчете НЦЗПИ, что подтверждается 5 актами и 3 справками.

Опубликование результатов диссертации

Основные положения диссертации отражены в 43 публикациях (общий объем 14,8 авторского листа), из них 9 статей (объем 6,3 авторского листа) опубликованы в изданиях, включенных в Перечень научных изданий Республики Беларусь для опубликования результатов диссертационных исследований, и иностранном научном издании; 9 статей – в сборниках научных статей, трудов, на электронных ресурсах; 25 публикаций – в сборниках материалов конференций и тезисов докладов.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, трех глав, объединяющих семь разделов, заключения, библиографического списка и приложений. Структура работы и логика изложения материала предопределены целью, задачами, объектом и предметом исследования. Общий объем диссертации составляет 291 страницу, в том числе текстовая часть на 193 страницах, библиографический список в количестве 393 наименований, включая 43 наименования публикаций соискателя, приводится на 41 странице, приложения занимают 57 страниц.

ОСНОВНАЯ ЧАСТЬ

Первая глава **«Становление и развитие уголовно-правовой охраны информационной безопасности»** состоит из двух разделов.

Раздел *1.1 «Аналитический обзор литературы по теме исследования»* посвящен исследованию взглядов на различные аспекты противодействия преступлениям против информационной безопасности и киберпреступлениям в теории уголовного права, а также в криминалистике и информационном праве. По данной и сходной тематике изучены работы Н.Ф. Ахраменка, Н.А. Бабия, А.В. Баркова, В.И. Берестеня, Г.А. Василевича, И.О. Грунтова, Е.Ф. Довгань, В.Ф. Ермоловича, М.А. Дубко, А.В. Дулова, Г.А. Зорина, Р.Н. Ключко, В.Е. Козлова, А.Н. Лепехина, В.В. Лосева, А.В. Макаревича, О.С. Макарова, Д.Г. Мороза, Н.О. Мороз, Э.Ф. Мичулиса, И.Г. Мухина, Д.В. Перевалова, А.С. Рубиса, Н.А. Савановича, А.Л. Савенка, С.А. Трахименка, В.В. Хилюты, В.М. Хомича, В.Б. Шабанова, Д.В. Шаблинской, А.А. Шардакова, Н.А. Швед, А.В. Шидловского, В.П. Шиенка, других белорусских и зарубежных ученых. Определены актуальные проблемы уголовно-правовой охраны информационной безопасности, которые остаются неизученными в науке уголовного права и представляют интерес для правоприменительной практики. Описаны методология, теоретическая и эмпирическая база диссертационного исследования.

В разделе *1.2 «Предпосылки установления уголовной ответственности за деяния, посягающие на информационную безопасность»* рассмотрены исторические причины и условия появления общественно опасных деяний, посягающих на информационную безопасность, а также эволюция норм, устанавливающих ответственность за их совершение, в национальном, зарубежном законодательстве и международном праве. Сделан научно обоснованный вывод о наличии определенных оснований для совершенствования норм УК с учетом развития регулятивного законодательства об информации, информатизации и защите информации и появления новых форм противоправных деяний, которым должна быть дана уголовно-правовая оценка (DDoS-атаки, незаконный оборот паролей и персональных данных и др.).

Вторая глава **«Информационная безопасность как объект уголовно-правовой охраны»** состоит из трех разделов.

В разделе *2.1 «Понятие информационной безопасности и роль уголовного закона в ее обеспечении»* на основании выявления автором статичного и динамичного аспектов рассмотрения информационной безопасности выделяются основные составляющие понятия информационной безопасности как объекта уголовно-правовой охраны (технологическая, гуманитарная, содержательная), формулируется его определение. Информация рассматривается в качестве предмета и средства совершения преступления. С учетом отнесения

компьютерной (цифровой) информации к системообразующим компонентам понятия кибербезопасности как видового объекта преступлений, предусмотренных гл. 31 УК, предлагается ее легальная дефиниция. В рамках динамичного аспекта информационной безопасности обосновывается вывод, что распространение отдельных видов информации негативного содержания представляет общественную опасность и имеет предпосылки для криминализации.

В разделе *2.2 «Понятие преступления против информационной безопасности»* исследуются различные способы описания преступлений, совершаемых в информационной сфере; с учетом статичного (предметного) и динамичного (содержательного) аспектов выделяются критерии отнесения общественно опасного деяния к преступлениям против информационной безопасности и предлагается его авторское определение. Аргументируется необходимость формулирования в уголовном законе «технически нейтральных» конструкций уголовно-правовых норм, охватывая возможность квалификации использования информационных технологий в рамках основного состава преступления.

В разделе *2.3 «Уголовно-правовая охрана гуманитарной составляющей информационной безопасности на примере защиты информации о частной жизни и персональных данных как вида информации ограниченного распространения»* детально исследуется в качестве предмета преступления такой вид информации ограниченного распространения, как информация о частной жизни и персональные данные, вне зависимости от формы ее закрепления. В целях обеспечения информационной безопасности личности обосновывается необходимость установления в виде материального состава преступления нормы об уголовной ответственности за незаконные действия с информацией о частной жизни и персональными данными, повлекшие причинение вреда правам, свободам и законным интересам потерпевшего.

В настоящее время уголовная ответственность предусмотрена только в отношении посягательств, касающихся информации о частной жизни, составляющих личную и семейную тайну, и не распространяется на защиту иных видов информации о частной жизни, в том числе на персональные данные. Поскольку персональные данные являются самостоятельной категорией информации ограниченного распространения, предлагается установить специальные нормы об ответственности за посягательства на них, что возможно путем как дополнения ст. 179 УК указанием на персональные данные, так и введения в перспективе специального состава преступления, направленного на защиту персональных данных.

Третья глава **«Уголовно-правовая охрана кибербезопасности (на примере разработки, использования либо распространения вредоносных**

программ) и направления ее усиления посредством криминализации новых угроз» содержит два раздела.

В разделе *3.1 «Уголовно-правовая характеристика разработки, использования либо распространения вредоносных программ»* проводится анализ состава преступления, предусмотренного ст. 354 УК; обосновываются предложения по совершенствованию его правовой конструкции и практики применения; осуществляется разграничение состава преступления, установленного ст. 354 УК, со смежными составами преступлений, предусмотренными УК.

В частности, разрабатываются направления совершенствования защиты от вредоносных компьютерных программ уголовно-правовыми средствами:

1) под вредоносной компьютерной программой следует понимать компьютерную программу, заведомо приводящую к несанкционированному уничтожению, блокированию, модификации либо копированию компьютерной (цифровой) информации, нарушению работы компьютерного оборудования, компьютерной (информационной) системы, сети или машинного носителя. В целях предотвращения избыточного употребления схожих терминов и системного изложения норм уголовного закона необходимо исключить деление вредоносных компьютерных программ на программы, предназначенные для несанкционированного уничтожения, блокирования, модификации или копирования информации, и специальные вирусные программы;

2) компьютерная (цифровая) информация может быть признана предметом преступления, в то время как сама специальная вирусная программа может рассматриваться не как предмет, а как средство совершения преступления, предусмотренного ст. 354 УК;

3) важен не сам процесс создания вредоносной компьютерной программы, а конечный результат ее создания, поэтому такое альтернативное действие, как внесение изменений в существующие программы, не несет в себе смысловой нагрузки и охватывается термином «разработка»;

4) в диспозиции ч. 1 ст. 354 УК следует непосредственно предусмотреть такие действия с самой вредоносной компьютерной программой, как ее предоставление (определенным лицам) и распространение (неопределенному кругу лиц);

5) термин «носители с такими программами» может быть исключен из диспозиции ч. 1 ст. 354 УК с учетом характера и степени общественной опасности подобного деяния;

6) альтернативные действия, предусмотренные в диспозиции ч. 1 ст. 354 УК, могут носить и правомерный характер (научно-исследовательская, образовательная работа, разрешенное испытание, оперативно-розыскная, контрразведывательная деятельность и иная деятельность в общественно

полезных целях). В связи с этим допустимо исключение из сферы действия ч. 1 ст. 354 УК законных случаев совершения указанного деяния;

7) применение в ч. 2 ст. 354 УК оценочного термина «тяжкие последствия» является обоснованным, однако в целях соблюдения правил юридической техники нуждается в согласовании с положениями ч. 3 ст. 349 УК;

8) в целях дифференциации уголовной ответственности с учетом правоприменительной практики и законодательного опыта других государств следует дополнить ст. 354 УК квалифицирующими признаками «группа лиц по предварительному сговору» и (или) «организованная группа», а также «угроза наступления тяжких последствий». Совершение рассматриваемого преступления в отношении КВОИ при отсутствии тяжких последствий может охватываться квалифицирующим признаком «угроза наступления тяжких последствий» и не требует отдельного выделения в силу специфики действующих норм законодательства об информации, информатизации и защите информации;

9) предложено исключить предусмотренную конструкцией субъективной стороны указанного преступления цель разработки компьютерной программы или внесения изменений в существующие программы, поскольку возможность несанкционированного уничтожения, блокирования, модификации или копирования информации – это объективное свойство вредоносной компьютерной программы, осознание которого формирует интеллектуальный элемент субъективной стороны преступления;

10) принимая во внимание направленность нормы ч. 2 ст. 354 УК, привлечение к уголовной ответственности возможно при наличии в действиях субъекта преступления неосторожной формы вины в отношении тяжких последствий (сложная вина). В силу большей общественной опасности умышленное причинение тяжких последствий должно квалифицироваться по совокупности ч. 1 ст. 354 УК и соответствующей статьи УК, предусматривающей ответственность за умышленное преступление;

11) санкция ч. 2 ст. 354 УК является чрезмерно строгой, не отвечает уголовно-правовому принципу справедливости, не согласуется с другими нормами гл. 31 УК, предусматривающими одинаковые общественно опасные последствия, в связи с чем подлежит смягчению.

В разделе *3.2 «Новые угрозы кибербезопасности: общественная опасность и возможность криминализации»* на основе объективных факторов проанализированы новые деяния, посягающие на кибербезопасность («спам», кибератаки (DDoS-атаки), незаконный оборот паролей, кодов доступа и иных аналогичных данных) на предмет допустимости установления уголовной ответственности за их совершение и разграничения со ст. 354 УК.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Проблема уголовно-правовой охраны общественных отношений в сфере обеспечения информационной безопасности, в том числе понятие преступления против информационной безопасности, в обозначенных в диссертации аспектах ранее комплексно не исследовалась [1; 7; 18].

В УК преступления против информационной безопасности рассматриваются в узком смысле – только как преступления против «кибербезопасности (компьютерной (цифровой) безопасности)». Вместе с тем понимание преступления против информационной безопасности в современных условиях не должно основываться только на использовании информационных технологий в преступных целях. Анализ норм УК и положений Концепции информационной безопасности позволяет сделать вывод, что кибербезопасность является составляющим технологическим элементом обеспечения информационной безопасности, но не единственным.

Выделены следующие составляющие понятия информационной безопасности как объекта уголовно-правовой охраны:

– кибербезопасность (компьютерная или цифровая безопасность) (защита компьютерной (цифровой) информации граждан, юридических лиц и иных организаций, компьютерной (цифровой) информации государственных органов, поддерживающей ее инфраструктуры, выступающих предметом преступления) – *технологическая составляющая*;

– защита информации (защита конфиденциальной информации (информации ограниченного распространения), в первую очередь информации о частной жизни и персональных данных, а также государственной, коммерческой, служебной и иной тайны, выступающих предметом преступления) – *гуманитарная составляющая*;

– защита интересов граждан, отдельных социальных групп, массовых объединений людей и общества в целом от воздействия информации, распространение которой запрещено законодательными актами (информация как средство совершения преступления независимо от формы ее представления), – *содержательная составляющая*;

– безусловная прерогатива государства в лице его органов и должностных лиц относительно защиты национальных интересов от «информационных войн».

В связи с этим в контексте решения задач уголовного закона понятие информационной безопасности автором рассматривается в двух аспектах: ***статичном*** (защита компьютерной (цифровой) информации и поддерживающей ее инфраструктуры (кибербезопасность как *технологическая составляющая информационной безопасности*), защита информации ограниченного

распространения, особенно информации о частной жизни и персональных данных, – *гуманитарная составляющая информационной безопасности*) и ***динамичном*** (защита от негативного воздействия информации).

Под информационной безопасностью в качестве объекта уголовно-правовой охраны соответствующих общественных отношений следует понимать состояние защищенности информации и поддерживающей ее инфраструктуры, а также законных интересов граждан, общества или отдельных его институтов, государства в информационной сфере от внешних и внутренних угроз, обеспечивающее ее формирование, функционирование и развитие во благо граждан, общества и государства [1, с. 91–92; 7; 15; 19; 23].

В статичном (предметном) аспекте преступления против информационной безопасности – это посягательства, направленные на саму информацию, компьютерные (информационные системы), сети, машинные и иные носители информации, технические устройства, связанные с обработкой информации, выступающие в рассматриваемом случае в качестве предмета преступления. При таком подходе к преступлениям против информационной безопасности полагаем целесообразным относить:

преступления, посягающие на компьютерную (цифровую) информацию и поддерживающую ее инфраструктуру (гл. 31 УК);

преступления, посягающие на информацию ограниченного распространения (например, ст. 178, 179, 203, 255, 373, 407 УК и др.).

В динамичном (содержательном) аспекте преступления против информационной безопасности – это преступления, связанные с публичным распространением информации, обращение которой в обществе запрещено и которая может причинить вред большому числу лиц.

В отличие от статичного (предметного) аспекта, отнесение указанных преступлений к преступлениям против информационной безопасности возможно не по основному, а обязательному дополнительному объекту преступления. Практическое значение такой классификации заключается в необходимости формирования четкого понимания способов и направленности совершения указанных преступлений, а также совершенствования юридической техники.

На основании выделения статичного (предметного) и динамичного (содержательного) аспектов исследуемой категории сформулировано авторское определение понятия ***«преступление против информационной безопасности»*** – общественно опасное противоправное виновное деяние, непосредственно посягающее на компьютерную (цифровую) информацию и поддерживающую ее инфраструктуру, правовой режим информации, распространение и (или) предоставление которой ограничено законодательными актами, а также сопряженное с распространением информации, обращение которой запрещено законодательными актами [1; 7; 12; 13; 15; 20; 32; 34].

2. В целях обеспечения единого понимания родового объекта преступлений против информационной безопасности и реализации положений Концепции национальной безопасности и Концепции информационной безопасности представляется обоснованным признание видовым объектом преступлений, предусмотренных гл. 31 УК, общественных отношений в сфере обеспечения ***кибербезопасности*** (компьютерной (цифровой) безопасности) как состояния защищенности информации в цифровой форме и поддерживающей ее инфраструктуры от любых угроз при использовании информационных технологий. В указанных целях необходимо также переосмысление преступлений против информационной безопасности в целом, наполнение их качественно новым содержанием, новеллами и составами преступлений, уже предусмотренными УК [1, с. 92; 5; 7; 13; 15; 20; 32].

Для устранения теоретических и практических противоречий относительно *технологической составляющей информационной безопасности*, имеющей первоочередное значение для действующих норм уголовного закона (гл. 31 УК), с учетом роли формы информации в современном обществе и построении цифрового государства, а также отнесения ее к системообразующим компонентам понятия кибербезопасности как отдельного объекта уголовно-правовой охраны, полагаем целесообразным предусмотреть в уголовном законе четкое определение понятия *компьютерной (цифровой) информации* как информации, хранящейся в компьютерной (информационной) системе, сети или на машинных носителях либо передаваемой в пространстве с помощью любых программно-технических средств. При этом понятие компьютерной (цифровой) информации охватывает понятие компьютерной программы [4; 6; 7; 26, с. 486; 32; приложения Д, Е к диссертации].

Независимо от формы представления информация может носить и динамичный характер, когда она является неотъемлемым элементом определенного действия и уже не предметом, а средством совершения преступления. Соответственно, в статике могут нарушаться интересы обладателя информации, в динамике – получателя. В контексте *динамичного аспекта преступления против информационной безопасности* (уголовно-правовая защита от информации) распространение отдельных видов информации негативного содержания (например, информации, побуждающей к причинению телесных повреждений, оправдывающей терроризм, отрицающей факты, установленные приговором Международного военного трибунала, образованного в соответствии с Лондонским соглашением от 8 августа 1945 г.), в том числе в глобальной компьютерной сети Интернет, имеет обоснованные предпосылки для криминализации [1; 7; 9, с. 39; 30; 34; 36].

3. Обеспечение кибербезопасности (компьютерной (цифровой) безопасности) средствами уголовного закона является одной из приоритетных и

актуальных задач для большинства современных государств, поскольку общественная опасность посягающих на нее преступлений заключается в непредсказуемых, зачастую необратимых последствиях, возможности незаконных действий в отношении различных видов информации, причинении вреда поддерживающей ее инфраструктуре, нарушении нормальной работы и деятельности граждан и организаций.

3.1. С учетом стремительного развития информационных технологий на фоне отставания механизмов выявления, раскрытия и предупреждения преступлений с их использованием требуется выработка эффективного и единого общемирового подхода к проблеме преступлений против информационной безопасности. На уровне охранительных правовых норм это может выражаться:

в совершенствовании норм национального уголовного и административного законодательства, касающихся конкретных составов правонарушений и преступлений против информационной безопасности;

в установлении минимального количества технических терминов и обеспечении их точности и однозначности при формулировании признаков составов преступлений против информационной безопасности с учетом развития информационных технологий и технических возможностей виновных лиц;

в закреплении единого универсального перечня преступлений против информационной безопасности [1; 7; 24; 34; 43];

3.2. В целях обеспечения стабильности уголовного закона и совершенствования юридической техники изложения его норм в случаях, когда это практически допустимо, предпочтительным является формулирование «технически нейтральных» конструкций уголовно-правовых норм, охватывая возможность квалификации использования современных информационных технологий в рамках основного, а не нового квалифицированного состава преступления [7; 9, с. 39; 43];

3.3. Незаконный оборот вредоносных компьютерных программ представляет общественную опасность и выступает одним из основных преступлений, посягающих на кибербезопасность [3, с. 738; 4; 22, с. 294–295]. В целях разрешения выявленных теоретических и практических проблем защиты от вредоносных компьютерных программ уголовно-правовыми средствами ст. 354 УК предложено изложить в следующей редакции:

«Статья 354. Незаконные разработка, использование, распространение либо предоставление вредоносной компьютерной программы

1. Незаконная разработка компьютерной программы, заведомо приводящей к несанкционированному уничтожению, блокированию, модификации либо копированию компьютерной (цифровой) информации, нарушению работы компьютерного оборудования, компьютерной (информационной) системы, сети

или машинного носителя (вредоносной компьютерной программы), либо незаконное заведомое ее использование, распространение, предоставление, –

наказываются штрафом, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. Те же действия, совершенные группой лиц по предварительному сговору либо создавшие угрозу наступления последствий, указанных в части 3 статьи 349 настоящего Кодекса, –

наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до шести лет.

3. Действия, предусмотренные частями 1 или 2 настоящей статьи, совершенные организованной группой либо повлекшие по неосторожности наступление последствий, указанных в части 3 статьи 349 настоящего Кодекса, –

наказываются ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от трех до семи лет.» [3–7; 21; 22; 27; 29; 31; 32; приложения Д, Е к диссертации];

3.4. С учетом существующих тенденций развития информационной сферы, зарубежного и международного опыта уголовно-правовой охраны технологического аспекта информационной безопасности – кибербезопасности (компьютерной (цифровой) безопасности) анализ таких новых угроз кибербезопасности, как «спам», кибератака (DoS- и DDoS-атака), незаконный оборот паролей (кодов) доступа, позволил произвести в рамках настоящего исследования их оценку на предмет возможной криминализации.

Кибератака (DoS- и DDoS-атака) связана с созданием препятствий для получения доступа законных пользователей к компьютерной (информационной) системе, как правило, сопровождается использованием и (или) распространением вредоносных компьютерных программ и является самостоятельным уголовно наказуемым деянием, поскольку представляет общественную опасность для граждан, общества и государства [6; 7; 17; 25]. Указанное деяние может быть рассмотрено как преступление против кибербезопасности и как преступление террористической или экстремистской направленности [6; 7; 9, с. 39; 17]. Отдельные кибератаки могут быть квалифицированы по ст. 351 УК. Однако действующие составы преступлений против информационной безопасности не в полной мере отражают существующую специфику DDoS-атак, не содержат все юридически значимые признаки их совершения [6; 7; 17].

Исходя из этого, ст. 351 УК предложено изложить в следующей редакции:

*«**Статья 351. Компьютерный саботаж***

1. Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной (цифровой) информации, либо вывод из строя компьютерного оборудования, либо разрушение, блокирование, нарушение работы компьютерной (информационной) системы, сети или машинного

носителя (компьютерный саботаж) –

наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от одного года до пяти лет.

2. Компьютерный саботаж, совершенный группой лиц по предварительному сговору, либо сопряженный с несанкционированным доступом к компьютерной (информационной) системе, сети или машинному носителю, либо создавший угрозу наступления последствий, указанных в части 3 статьи 349 настоящего Кодекса, –

наказывается ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от двух до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Компьютерный саботаж, совершенный организованной группой либо повлекший последствия, указанные в части 3 статьи 349 настоящего Кодекса, –

наказывается лишением свободы на срок от трех до десяти лет.» [6; 7; 11; 17; 28; 32; приложения Д, Е к диссертации];

3.5. Незаконные действия с паролями представляют общественную опасность, категоризированы как преступления в международном праве и зарубежном законодательстве. Учитывая отсутствие мер правового воздействия на лиц, занимающихся незаконным оборотом паролей в Республике Беларусь, мировые тенденции консолидации усилий государств в борьбе с преступлениями против информационной безопасности и унификации норм материального уголовного права с положениями международных договоров, необходимо установить уголовную ответственность за отдельные действия с паролями и в Республике Беларусь, дополнив гл. 31 УК ст. 353[1] следующего содержания:

«Статья 353[1]. Незаконные изготовление, приобретение либо сбыт паролей, кодов доступа или иных аналогичных данных

Незаконные изготовление с целью сбыта, приобретение либо сбыт паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к защищенному машинному носителю, защищенной компьютерной (информационной) системе или сети в целом или любой их части для совершения преступлений, предусмотренных статьями 179, 203, 212, 254, 349–352 настоящего Кодекса, –

наказываются штрафом, или арестом, или ограничением свободы на срок до двух лет.» [6; 7; 11; 28; 39; 42; приложения Д, Е к диссертации];

3.6. Распространение «спама» является самостоятельным противоправным деянием, посягающим на информационную безопасность (кибербезопасность), отличным от иных преступлений против информационной

безопасности по своему содержанию и направленности, не имеющим в настоящее время достаточных предпосылок для криминализации в связи с отсутствием существенного вреда, присущего преступлению, либо возможности его причинения. После закрепления критериев определения понятия «спам» в регулятивном законодательстве в целях защиты и предупреждения совершения иных противоправных деяний в информационной сфере может быть рассмотрен вопрос установления мер административной ответственности за различные виды «спама» [6; 7; 10; 11; 28].

4. Принимая во внимание *гуманитарную составляющую информационной безопасности*, предполагающую, что конфиденциальная информация может выступать предметом преступления, и авторский подход к определению преступления против информационной безопасности, с учетом характера и степени общественной опасности деяния имеются предпосылки установления уголовной ответственности за незаконные действия с информацией о частной жизни (в широком смысле, включающем не только личную и семейную тайну) и персональными данными как самостоятельными категориями информации ограниченного распространения в виде материального состава преступления, предусматривающего причинение вреда правам, свободам и законным интересам потерпевшего [2, с. 730; 7; 8; 14; 16; 33; 37; 40]. Незаконные действия в отношении информации о частной жизни и персональных данных при отсутствии общественно опасных последствий, а также нарушение прав субъектов персональных данных (на получение информации об обработке персональных данных и др.), правил защиты персональных данных должны влечь административную ответственность [2; 7; 8; 37; 40].

Исходя из указанного, предложено согласовать ст. 179 УК с нормами законодательства об информации, информатизации и защите информации, изложив ее в следующей редакции:

«Статья 179. Незаконные сбор, обработка, распространение либо предоставление информации о частной жизни и персональных данных

1. Умышленные незаконные сбор, обработка, распространение либо предоставление информации о частной жизни и (или) персональных данных другого лица без его согласия, повлекшие причинение вреда правам, свободам и законным интересам потерпевшего, –

наказываются общественными работами, или штрафом, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. Те же действия, совершенные с использованием специальных технических средств, предназначенных для негласного получения информации, либо лицом в связи с его профессиональной или служебной деятельностью, либо лицом, достигшим восемнадцатилетнего возраста, в отношении заведомо несовершеннолетнего, –

наказываются лишением права занимать определенные должности или заниматься определенной деятельностью со штрафом, либо ограничением свободы на срок до пяти лет со штрафом, либо лишением свободы на тот же срок со штрафом.» [2, с. 730; 7; 8; 16; 33; 35; 37; 40; 41; приложения Д, Е к диссертации].

5. Системный характер изучения информационной безопасности как объекта уголовно-правовой охраны позволил сформулировать рекомендации по практическому применению исследуемых норм уголовного закона и квалификации соответствующих деяний:

– допускается квалификация противоправного использования информационных технологий при отсутствии прямого указания на их использование в конкретных нормах Особенной части УК [7; 9, с. 39; 43];

– совершение незаконных действий с информацией о частной жизни и персональными данными, отображенной в форме компьютерной (цифровой) информации, влечет ответственность по совокупности преступлений с соответствующими преступлениями, предусмотренными гл. 31 УК. Если информация о частной жизни или персональные данные являются составной частью иной информации ограниченного распространения (например, государственных секретов, материалов уголовного дела и др.), деяние должно квалифицироваться по статье УК, предусматривающей ответственность за посягательство на указанную категорию информации ограниченного распространения [2, с. 729–730; 8];

– разработка вредоносной компьютерной программы включает в себя разработку специальной вирусной программы и может быть признана оконченной при наличии следующих условий: 1) компьютерная программа зафиксирована на материальном носителе в форме, доступной для восприятия техническими средствами (устройствами); 2) в алгоритме компьютерной программы содержится вредоносный код [4; 27; 31, с. 357; 38, с. 550];

– время окончания использования специальных вирусных программ связано с началом контролируемого преступником их применения в информационных системах, сетях, машинных носителях, устройствах для определенных целей [4; 38, с. 550];

– окончанием распространения носителей с вредоносными компьютерными программами является момент вовлечения их в гражданский оборот в виде отчуждения в любой форме, а моментом окончания распространения вредоносной компьютерной программы в глобальной или локальной компьютерной сети – время ее размещения на определенном информационном ресурсе, в информационной системе, на сервере или устройстве, ином машинном носителе посредством удаленного доступа [4; 38, с. 550];

– носителем с вредоносными компьютерными программами является материальный объект (жесткий диск, Flash-накопитель, мобильный телефон (смартфон) и др.), используемый для хранения и отображения информации, в том числе в виде вредоносной компьютерной программы [3, с. 746; 12; 21];

– в случае уничтожения, блокирования, модификации либо копирования компьютерной (цифровой) информации, нарушения работы компьютерного оборудования, компьютерной (информационной) системы или сети, а также заведомого наступления тяжких последствий распространение носителей с вредоносными компьютерными программами (диски, Flash-накопители, смартфоны и др.) должно квалифицироваться по ч. 1 ст. 354 УК (распространение, предоставление или использование вредоносной компьютерной программы) и статьям УК, связанным с наступлением соответствующих последствий [4; 5; 29];

– в качестве «тяжких последствий», кроме указанных в ч. 3 ст. 349 УК, применительно к преступлениям против информационной безопасности (кибербезопасности) можно считать также причинение вреда КВОИ или объектам, которые подлежат отнесению к ним в порядке, предусмотренном законодательством [5; 6];

– квалификация кибератаки как деяния, образующего объективную сторону акта терроризма (международного терроризма) или диверсии, при наличии уголовно-правовых признаков является допустимой и соответствует положениям Концепции информационной безопасности [6; 7; 9, с. 39; 17].

Рекомендации по практическому использованию результатов

Результаты исследования могут быть использованы государственными органами при разработке законопроектов, направленных на совершенствование уголовного законодательства (справки Постоянной комиссии Палаты представителей Национального собрания Республики Беларусь по национальной безопасности, Следственного комитета Республики Беларусь), в их правоприменительной деятельности (справки Оперативно-аналитического центра при Президенте Республики Беларусь, Следственного комитета Республики Беларусь), а также внедрены в законотворческую деятельность (акты НЦЗПИ), научно-исследовательскую работу (акт Института правовых исследований НЦЗПИ), образовательный процесс учреждений образования (акты УО «Академия Министерства внутренних дел Республики Беларусь», УО «Белорусский государственный экономический университет»).

Выводы и научные положения, сформулированные в диссертации, могут послужить основой для последующих исследований по вопросам уголовно-правовой охраны информационной безопасности.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ

Статьи в научных изданиях, включенных ВАК в перечень изданий для опубликования результатов диссертационного исследования

1. Полещук, Д. Г. Понятие и объект преступления против информационной безопасности / Д. Г. Полещук // Право.by. – 2016. – № 6. – С. 87–92.

2. Полещук, Д. Г. Уголовно-правовая охрана информации ограниченного распространения на примере информации о частной жизни и персональных данных / Д. Г. Полещук // Право в современном белорусском обществе : сб. науч. тр. / Нац. центр законодательства и правовых исслед. Респ. Беларусь, Ин-т правовых исслед. – Минск, 2017. – Вып. 12 : Юбилейн. сб. науч. тр., посвящ. 20-летию Нац. центра законодательства и правовых исслед. Респ. Беларусь. – С. 722–730.

3. Полещук, Д. Г. Разработка, использование либо распространение вредоносных программ: проблема предмета преступления / Д. Г. Полещук // Право в современном белорусском обществе : сб. науч. тр. / Нац. центр законодательства и правовых исслед. Респ. Беларусь, Ин-т правовых исслед. – Минск, 2018. – Вып. 13 : Посвящ. д-ру юрид. наук, проф., заслуж. юристу Респ. Беларусь С. Г. Дробязко. – С. 738–746.

4. Полещук, Д. Г. Объективные признаки уголовной противоправности незаконных действий с вредоносными компьютерными программами как преступления против кибербезопасности / Д. Г. Полещук // Право.by. – 2019. – № 5. – С. 100–105.

5. Полещук, Д. Г. Отдельные направления совершенствования правовой конструкции статьи 354 Уголовного кодекса Республики Беларусь («Разработка, использование либо распространение вредоносных программ») / Д. Г. Полещук // Юстиция Беларуси. – 2019. – № 11. – С. 69–74.

6. Полещук, Д. Г. Совершенствование уголовно-правовых средств охраны кибербезопасности в Республике Беларусь / Д. Г. Полещук // Право в современном белорусском обществе : сб. науч. тр. / Нац. центр законодательства и правовых исслед. Респ. Беларусь, Ин-т правовых исслед. – Минск, 2019. – Вып. 14. – С. 555–565.

7. Полещук, Д. Г. Уголовно-правовая охрана информационной безопасности: отдельные теоретические и практические аспекты / Д. Г. Полещук // Вопросы криминологии, криминалистики и судебной экспертизы : сб. науч. тр. / Науч.-практ. центр Гос. ком. судеб. экспертиз Респ. Беларусь. – Минск, 2019. – Вып. 2. – С. 56–63.

8. Полещук, Д. Г. Некоторые аспекты уголовно-правовой охраны информационной безопасности на примере защиты информации о частной жизни

и персональных данных / Д. Г. Полещук // Юстиция Беларуси. – 2020. – № 1. – С. 25–30.

Статьи в иностранных научных изданиях

9. Полещук, Д. Г. Противодействие экстремизму в сети «Интернет»: охранительный аспект / Д. Г. Полещук // Информ. право. – 2019. – № 1. – С. 35–39.

Статьи в сборниках научных статей, трудов, на электронных ресурсах

10. Полещук, Д. Г. К вопросу об установлении ответственности за спам / Д. Г. Полещук // Проблемы правотворческой и правоприменительной практики в условиях развития информационного общества : сб. науч. ст. : в 2 ч. / Гродн. гос. ун-т ; редкол.: С. Е. Чебуранова (гл. ред.) [и др.]. – Гродно, 2015. – Ч. 1. – С. 170–174.

11. Полещук, Д. Г. Информационные технологии и уголовное право: грани взаимодействия и оценка возможности криминализации отдельных деяний / Д. Г. Полещук // Актуальные проблемы уголовного законодательства на современном этапе : сб. науч. тр. междунар. науч.-практ. конф., Волгоград, 14–15 мая 2015 г. / Волгогр. акад. МВД России ; отв. ред. В. И. Третьяков. – Краснослободск, 2015. – С. 294–300.

12. Полещук, Д. Г. Применение информационных технологий в сфере реализации норм уголовного права [Электронный ресурс] / Д. Г. Полещук // Информационные технологии и право (Правовая информатизация – 2015) : материалы V Междунар. науч.-практ. конф., Минск, 28 мая 2015 г. / Нац. центр правовой информ. Респ. Беларусь ; под общ. ред. Е. И. Коваленко. – Минск, 2015. – 1 электрон. опт. диск (CD-ROM).

13. Полещук, Д. Г. Уголовно-правовая охрана общественных отношений в сфере обеспечения информационной безопасности / Д. Г. Полещук // Научно-образовательное пространство стран СНГ: история, достижения, потенциал : сб. ст. из материалов Евраз. науч. форума, 25 дек. 2015 г. : [в 2 ч.] / С.-Петерб. науч. центр Рос. акад. наук [и др.] ; общ. науч. ред. М. Ю. Спириной. – СПб., 2016. – Ч. 2. – С. 103–108.

14. Полещук, Д. Г. Уголовная ответственность за нарушение законодательства о персональных данных в Российской Федерации и зарубежных государствах: сравнительно-правовой анализ / Д. Г. Полещук // Уголовный кодекс Российской Федерации: современное состояние и перспективы развития (к 20-летию принятия) : сб. ст. / Гос. гуманитар.-технол. ун-т [и др.] ; редкол.: С. А. Маркунцов (отв. ред.) [и др.]. – М., 2016. – С. 136–143.

15. Полещук, Д. Г. Понятие информационной безопасности в законодательстве Республики Беларусь / Д. Г. Полещук // Конституционные права и свободы: проблемы интерпретации и реализации в национальных правовых

системах : сб. ст. междунар. науч.-практ. конф., Новополоцк, 28–29 окт. 2016 г. : в 3 т. / Полоц. гос. ун-т, Регион. учеб.-науч.-практ. Юрид. центр ; редкол.: И. В. Вегера (отв. ред.) [и др.]. – Новополоцк, 2016. – Т. 1. – С. 251–256.

16. Полещук, Д. Г. К вопросу об уголовной ответственности за незаконные действия в отношении информации о частной жизни и персональных данных / Д. Г. Полещук // Актуальные проблемы совершенствования уголовного законодательства Республики Беларусь на современном этапе : сб. науч. ст. / Нац. центр законодательства и правовых исслед. Респ. Беларусь. – Минск, 2016. – Вып. 2 : Посвящ. 80-летию проф. Э. А. Саркисовой. – С. 176–184.

17. Полещук, Д. Г. Уголовная ответственность за совершение компьютерных атак / Д. Г. Полещук // Актуальные проблемы совершенствования уголовного законодательства Республики Беларусь на современном этапе : сб. науч. ст. / Нац. центр законодательства и правовых исслед. Респ. Беларусь. – Минск, 2017. – Вып. 3 : Посвящ. 80-летию проф. Э. Ф. Мичулиса. – С. 205–215.

18. Полещук, Д. Г. Уголовно-правовая охрана общественных отношений в сфере обеспечения информационной безопасности Республики Беларусь: история и современность / Д. Г. Полещук // 20 лет Уголовному кодексу Республики Беларусь: проблемы применения и направления совершенствования : сб. науч. ст. / Нац. центр законодательства и правовых исслед. Респ. Беларусь ; редкол.: И. И. Лапцевич (отв. ред.) [и др.]. – Минск, 2019. – С. 129–141.

Материалы конференций, тезисы докладов

19. Полещук, Д. Г. Понятие информационной безопасности / Д. Г. Полещук // Актуальные вопросы современной правовой науки : материалы Междунар. науч. конф. студентов, магистрантов и аспирантов и секции «Юридические науки» Респ. науч. конф. студентов и аспирантов вузов Респ. Беларусь «НИРС – 2011», Минск, 4–5 нояб. 2011 г. / Белорус. гос. ун-т ; редкол.: О. И. Чуприс (отв. ред.) [и др.]. – Минск, 2012. – С. 52–53.

20. Полещук, Д. Г. Некоторые уголовно-правовые аспекты преступлений против информационной безопасности / Д. Г. Полещук // Юридическая наука и правоприменительная практика : материалы Междунар. науч. конф. студентов, магистрантов и аспирантов, Минск, 26–27 окт. 2012 г. / Белорус. гос. ун-т ; редкол.: О. И. Чуприс (отв. ред.) [и др.]. – Минск, 2012. – С. 200–201.

21. Полещук, Д. Г. Уголовно-правовая защита от вредоносных компьютерных программ в Республике Беларусь / Д. Г. Полещук // Молодежная инициатива в решении современных проблем юриспруденции : материалы междунар. науч. конф. студентов, магистрантов и аспирантов, Минск, 25–26 окт. 2013 г. / Белорус. гос. ун-т ; редкол.: Т. А. Червякова (отв. ред.) [и др.]. – Минск, 2013. – С. 167–168.

22. Полещук, Д. Г. Разработка, использование либо распространение вредоносных программ (статья 354 УК Республики Беларусь): некоторые аспекты / Д. Г. Полещук // Сборник работ 71-й научной конференции студентов и аспирантов Белорусского государственного университета, Минск, 18–21 мая 2014 г. : в 3 ч. / Белорус. гос. ун-т. – Минск, 2014. – Ч. 2. – С. 294–296.

23. Полещук, Д. Г. Роль СМИ в предупреждении расовой, национальной и религиозной нетерпимости и острых конфликтов на этой почве / Д. Г. Полещук // Партнерство государства, общественного сектора и делового сообщества в борьбе с терроризмом – безопасность через диалог, согласие и взаимодействие : материалы междунар. науч.-практ. конф., Минск, 30–31 окт. 2014 г. : в 2 т. / Ин-т нац. безопасности Респ. Беларусь ; редкол.: С. Н. Князев (гл. ред.) [и др.]. – Минск, 2014. – Т. 1. – С. 172–175.

24. Полещук, Д. Г. Основные тенденции развития киберпреступности в современном мире / Д. Г. Полещук // Актуальные проблемы криминологического исследования региональной преступности : материалы II междунар. науч.-практ. конф., Баку, 21 окт. 2014 г. / Акад. полиции МВД Азерб. Респ. ; редкол.: А. Феттахова (отв. ред.) [и др.]. – Баку, 2015. – С. 365–372.

25. Полещук, Д. Г. DDOS-атака: уголовно наказуемое деяние или легальный протест? / Д. Г. Полещук // Право и государство: история, современность, перспективы развития : материалы междунар. науч. конф. студентов, магистрантов и аспирантов, Минск, 24–25 окт. 2014 г. / Белорус. гос. ун-т ; редкол.: Т. А. Червякова (отв. ред.) [и др.]. – Минск, 2015. – С. 213–215.

26. Полещук, Д. Г. Понятие компьютерной информации и его значение в уголовно-правовом обеспечении информационной безопасности / Д. Г. Полещук // Молодежь и наука: реальность и будущее : материалы VIII междунар. науч.-практ. конф. : в 2 т. / Невинномыс. ин-т экономики, упр. и права ; редкол.: Т. Н. Рябченко, Е. И. Бурьянова. – Невинномысск, 2015. – Т. 2. – С. 485–486.

27. Полещук, Д. Г. Отдельные аспекты разработки вредоносных программ / Д. Г. Полещук // Сборник работ 72-й научной конференции студентов и аспирантов Белорусского государственного университета, Минск, 11–22 мая 2015 г. : в 3 ч. / Белорус. гос. ун-т. – Минск, 2015. – Ч. 3. – С. 186–188.

28. Poleshchuk, D. G. Information technology and criminal law: the possibility of certain acts criminalization / D. G. Poleshchuk // Сборник работ 72-й научной конференции студентов и аспирантов Белорусского государственного университета, Минск, 11–22 мая 2015 г. : в 3 ч. / Белорус. гос. ун-т. – Минск, 2015. – Ч. 3. – С. 189–191.

29. Полещук, Д. Г. Анализ санкции преступления, предусмотренного ст. 354 Уголовного кодекса Республики Беларусь / Д. Г. Полещук // Актуальные вопросы уголовно-исполнительного права, криминологии и исполнения наказаний :

междунар. науч.-практ. конф., Минск, 28 мая 2015 г. : тез. докл. / Акад. МВД Респ. Беларусь ; редкол.: В. Б. Шабанов (отв. ред.) [и др.]. – Минск, 2015. – С. 140–142.

30. Полещук, Д. Г. Интернет-груминг: понятие и оценка возможности криминализации / Д. Г. Полещук // Теоретико-методологические и конституционные основы устойчивого развития национальной правовой системы в условиях глобальных и региональных процессов в контексте защиты прав человека и построения правового государства : материалы Междунар. науч.-практ. конф., посвящ. 90-летию юрид. фак. БГУ, Минск, 19–20 окт. 2015 г. / Белорус. гос. ун-т [и др.] ; редкол.: С. А. Балашенко (гл. ред.), С. А. Калинин, О. Ю. Ширинский. – Минск, 2015. – С. 521–523.

31. Полещук, Д. Г. Разработка теоретических положений по совершенствованию объективной стороны преступления, предусмотренного ст. 354 Уголовного кодекса Республики Беларусь / Д. Г. Полещук // Теоретические и прикладные аспекты современной юридической науки : сб. материалов междунар. науч.-практ. конф., посвящ. памяти проф. В. И. Семенкова, Минск, 11 дек. 2015 г. / Нац. центр законодательства и правовых исслед. Респ. Беларусь ; редкол.: С. М. Сивец [и др.]. – Минск, 2015. – С. 355–357.

32. Полещук, Д. Г. Проблемы понимания и использования терминов при формулировании и уяснении признаков составов преступлений против информационной безопасности / Д. Г. Полещук // Теоретические и прикладные аспекты информационной безопасности : материалы междунар. науч.-практ. конф., Минск, 31 марта 2016 г. / Акад. МВД Респ. Беларусь ; редкол.: А. В. Яскевич (отв. ред.) [и др.]. – Минск, 2016. – С. 119–122.

33. Полещук, Д. Г. Ответственность за незаконное собирание и распространение персональных данных / Д. Г. Полещук // Проблемы борьбы с преступностью и подготовки кадров для правоохранительных органов : Междунар. науч.-практ. конф., Минск, 7 апр. 2016 г. : тез. докл. / Акад. МВД Респ. Беларусь ; редкол.: А. В. Яскевич (отв. ред.) [и др.]. – Минск, 2016. – С. 139–140.

34. Полещук, Д. Г. Международные стандарты уголовно-правовой защиты прав человека в информационной сфере / Д. Г. Полещук // Идеал свободной человеческой личности: от международных пактов о правах человека к современной конституции : междунар. науч.-практ. конф., Минск, 16 дек. 2016 г. : тез. докл. / Акад. МВД Респ. Беларусь ; редкол.: А. В. Яскевич (отв. ред.) [и др.]. – Минск, 2016. – С. 143–145.

35. Полещук, Д. Г. Уголовная ответственность за незаконные действия с персональными данными / Д. Г. Полещук // Общество, государство, право: тенденции и перспективы развития : материалы междунар. науч. конф. студентов, магистрантов и аспирантов, Минск, 21–22 окт. 2016 г. / Белорус. гос. ун-т ; редкол.: Т. А. Червякова (отв. ред.) [и др.]. – Минск, 2017. – С. 209–210.

36. Полещук, Д. Г. Ответственность за распространение отдельных видов информации негативного содержания / Д. Г. Полещук // Проблемы борьбы с преступностью и подготовки кадров для правоохранительных органов : Междунар. науч.-практ. конф., посвящ. 100-летию милиции Беларуси, Минск, 10 февр. 2017 г. : тез. докл. / Акад. МВД Респ. Беларусь ; редкол.: А. В. Яскевич (отв. ред.) [и др.]. – Минск, 2017. – С. 191–192.

37. Полещук, Д. Г. Проблемы объективной стороны преступления, предусмотренного ст. 179 УК / Д. Г. Полещук // Вклад молодых ученых в развитие правовой науки Республики Беларусь : сб. материалов VI Междунар. науч. конф., Минск, 2 июня 2017 г. / Нац. центр законодательства и правовых исслед. Респ. Беларусь ; редкол. С. М. Сивец [и др.]. – Минск, 2017. – С. 338–342.

38. Полещук, Д. Г. Время окончания преступления, предусмотренного ст. 354 Уголовного кодекса Республики Беларусь / Д. Г. Полещук // Научные чтения памяти профессора В. И. Семенкова : сб. материалов Респ. науч.-практ. конф. с междунар. участием, Минск, 7 дек. 2017 г. / Нац. центр законодательства и правовых исслед. Респ. Беларусь ; редкол.: С. М. Сивец [и др.]. – Минск, 2017. – С. 546–550.

39. Полещук, Д. Г. Незаконный оборот паролей, кодов доступа к компьютерной системе, сети или машинному носителю: перспективы криминализации / Д. Г. Полещук // Теоретические и прикладные проблемы информационной безопасности : материалы Междунар. науч.-практ. конф., Минск, 18 мая 2017 г. / Акад. МВД Респ. Беларусь ; редкол.: А. В. Яскевич (отв. ред.) [и др.]. – Минск, 2018. – С. 56–59.

40. Полещук, Д. Г. Защита персональных данных в условиях развития цифровой экономики: охранительный аспект / Д. Г. Полещук // Стратегия развития экономики Беларуси: вызовы, инструменты реализации и перспективы : материалы Междунар. науч.-практ. конф., Минск, 20–21 сент. 2018 г. : в 2 т. / НАН Беларуси, Ин-т экономики ; редкол.: В. И. Бельский [и др.]. – Минск, 2018. – Т. 2. – С. 323–325.

41. Полещук, Д. Г. Субъективные признаки незаконных действий в отношении информации о частной жизни и персональных данных: некоторые аспекты / Д. Г. Полещук // Вклад молодых ученых в развитие правовой науки Республики Беларусь : сб. материалов VII Респ. науч. конф., Минск, 15 нояб. 2018 г. / Нац. центр законодательства и правовых исслед. Респ. Беларусь ; редкол.: С. М. Сивец [и др.]. – Минск, 2018. – С. 243–246.

42. Полещук, Д. Г. Уголовная ответственность за незаконный оборот паролей (кодов) доступа к компьютерной системе, сети или машинному носителю / Д. Г. Полещук // Информационная революция и вызовы новой эпохи – стимулы формирования современных подходов к информационной безопасности : материалы междунар. науч.-практ. конф., Минск, 29–30 нояб. 2018 г. : в 2 т. / Ин-т

нац. безопасности Респ. Беларусь ; редкол.: С. Н. Князев (гл. ред.) [и др.]. – Минск, 2019. – Т. 2. – С. 133–137.

43. Полещук, Д. Г. Современные информационные технологии и их отражение в нормах уголовного права / Д. Г. Полещук // Конституция Республики Беларусь как ценностный выбор: 25 лет свершений и преобразований : сб. материалов Респ. науч.-практ. конф., Минск, 4 марта 2019 г. / Белорус. гос. ун-т [и др.] ; редкол.: Г. А. Василевич (гл. ред.) [и др.]. – Минск, 2019. – С. 325–328.

РЭЗЮМЭ

Палешчук Дзмітрый Рыгоравіч

КРЫМІНАЛЬНА-ПРАВАВАЯ АХОВА ІНФАРМАЦЫЙНАЙ БЯСПЕКІ (НА ПРЫКЛАДЗЕ АСОБНЫХ АСПЕКТАЎ АХОВЫ КІБЕРБЯСПЕКІ І АБАРОНЫ ІНФАРМАЦЫІ АБМЕЖАВАНАГА РАСПАЎСЮДЖВАННЯ)

Ключавыя словы: крымінальны закон, інфармацыйная бяспека, кібербяспека, камп'ютарная інфармацыя, персанальныя даныя, шкоднасная камп'ютарная праграма.

Мэта даследавання: распрацоўка тэарэтыка-прававых асноў крымінальна-прававой аховы інфармацыйнай бяспекі, а таксама прапаноў па ўдасканаленні крымінальнага закона і практыкі яго прымянення ў частцы адказнасці за замахі на грамадскія адносіны з нагоды забеспячэння інфармацыйнай бяспекі, кібербяспекі і абароны інфармацыі абмежаванага распаўсюджвання.

Метады даследавання: аснову складае дыялектычны метад, выкарыстаны агульнанавуковыя, спецыяльныя і прыватныя метады: аналіз і сінтэз, індукцыя і дэдукцыя, абстрагаванне і абагульненне, статыстычны, канкрэтна-сацыялагічны, метад тлумачэння права, параўнальна-прававы, гісторыка-прававы, фармальна-юрыдычны, прагнастычны.

Атрыманыя вынікі і навізна: праведзена комплекснае даследаванне паняцця злачынства супраць інфармацыйнай бяспекі. Прадстаўлены новыя навукова абгрунтаваныя вывады і прапановы па ўдасканаленні крымінальна-прававой аховы інфармацыйнай бяспекі: вызначэнне камп'ютарнай (лічбавай) інфармацыі, новая рэдакцыя арт. 354 КК; спецыяльная норма аб крымінальнай адказнасці за незаконныя дзеянні з персанальнымі данымі пры наяўнасці грамадска небяспечных наступстваў; аналіз новых дзеянняў, якія пасягаюць на кібербяспеку (распаўсюджванне «спаму», кібератака, незаконны абарот пароляў (кодаў) доступу); абгрунтаванне абароны ад інфармацыі негатыўнага зместу крымінальна-прававымі сродкамі.

Рэкамендацыі па выкарыстанні: вывады і прапановы па пытаннях крымінальна-прававой аховы інфармацыйнай бяспекі могуць быць выкарыстаны пры ўдасканальванні заканадаўства, у правапрымяняльнай дзейнасці, адукацыйным працэсе, паслужыць асновай для правядзення далейшых даследаванняў па дадзенай праблематыцы.

Галіна прымянення: праватворчая і правапрымяняльная дзейнасць, навуковыя даследаванні, адукацыйны працэс.

РЕЗЮМЕ

Полещук Дмитрий Григорьевич

УГОЛОВНО-ПРАВОВАЯ ОХРАНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (НА ПРИМЕРЕ ОТДЕЛЬНЫХ АСПЕКТОВ ОХРАНЫ КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ)

Ключевые слова: уголовный закон, информационная безопасность, кибербезопасность, компьютерная информация, персональные данные, вредоносная компьютерная программа.

Цель исследования: разработка теоретико-правовых основ уголовно-правовой охраны информационной безопасности, а также предложений по совершенствованию уголовного закона и практики его применения в части ответственности за посягательства на общественные отношения по поводу обеспечения информационной безопасности, кибербезопасности и защиты информации ограниченного распространения.

Методы исследования: основу составляет диалектический метод, использованы общенаучные, специальные и частные методы: анализ и синтез, индукция и дедукция, абстрагирование и обобщение, статистический, конкретно-социологический, метод толкования права, сравнительно-правовой, историко-правовой, формально-юридический, прогностический.

Полученные результаты и новизна: проведено комплексное исследование понятия преступления против информационной безопасности. Представлены новые научно обоснованные выводы и предложения по совершенствованию уголовно-правовой охраны информационной безопасности: определение компьютерной (цифровой) информации, новая редакция ст. 354 УК; специальная норма об уголовной ответственности за незаконные действия с персональными данными при наличии общественно опасных последствий; анализ новых деяний, посягающих на кибербезопасность (распространение «спама», кибератака, незаконный оборот паролей (кодов) доступа); обоснование защиты от информации негативного содержания уголовно-правовыми средствами.

Рекомендации по использованию: выводы и предложения по вопросам уголовно-правовой охраны информационной безопасности могут быть использованы при совершенствовании законодательства, в правоприменительной деятельности, образовательном процессе, послужить основой для проведения дальнейших исследований по данной проблематике.

Область применения: правотворческая и правоприменительная деятельность, научные исследования, образовательный процесс.

RESUME

Poleshchuk Dmitriy Grigorievich

CRIMINAL LEGAL PROTECTION OF INFORMATION SECURITY (ON THE EXAMPLE OF SEPARATE ASPECTS OF CYBERSECURITY PROTECTION AND PROTECTION OF INFORMATION OF LIMITED DISSEMINATION)

Key words: criminal law, information security, cybersecurity, computer information, personal data, malicious computer program.

The purpose of the work: development of the theoretical and legal foundations of the criminal legal protection of information security, as well as proposals to improve the criminal law and the practice of its application in terms of responsibility for encroachments on public relations in relation to ensuring information security, cybersecurity and the protection of information of limited dissemination.

Methods of research: the basis is the dialectical method; general scientific, special and particular methods are used: analysis and synthesis, induction and deduction, abstraction and generalization, statistical, concrete sociological, method of interpretation of law, comparative legal, historical legal, formal legal, prognostic.

The results obtained and novelty: conducted a comprehensive study of the concept of crime against information security. New scientifically based conclusions and proposals for improving the criminal law protection of information security are presented: definition of computer (digital) information, new edition of Art. 354 of the Criminal Code; special norm on criminal liability for illegal actions with personal data in the presence of socially dangerous consequences; assessment of new acts encroaching on cybersecurity (spamming, cyber attack, illegal traffic of access passwords (codes); justification for protecting from information of negative content by criminal law means.

Recommendations for the use: conclusions and suggestions on the criminal law protection of information security can be used to improve legislation, in law enforcement, the educational process, serve as the basis for further research on this issue.

The sphere of application: law-making and law enforcement, research, educational process.

Подписано в печать 14.10.2020 г. Формат 60х84/16. Бумага офсетная.
Печать офсетная. Усл. печ. л. 1,86. Уч.-изд. л. 1,64.
Тираж 60 экз. Заказ 381.

Республиканское унитарное предприятие «Информационно-
вычислительный центр Министерства финансов Республики Беларусь».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий
№2/41 от 29.01.2014.
Ул. Кальварийская, 17, 220004, г. Минск.