DOI: 10.7256/1811-9018.2015.4.14776
При цитировании этой статьи сноска на doi обязательна

§ 10 ПРАВОВЕДЕНИЕ

Степанов-Егиянц В.Г.

ПОНЯТИЙНО-ТЕРМИНОЛОГИЧЕСКИЕ ОСНОВЫ БЕЗОПАСНОГО ОБРАЩЕНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В УГОЛОВНО-ПРАВОВОМ АСПЕКТЕ

Аннотация: *Предметом исследования является проблема формирования понятийно-терминологического аппарата в сфере безопасного обращения компьютерной информации в уголовно-правовом аспекте. Исследуются такие поняти я как кибернетика, информационное пространство, компьютерное преступление, киберпреступность, информационно-теологический террористический акт, информационная угроза, информационная атака и т.п. Исследуются примеры использования подобной терминологии в зарубежном уголовном законодательстве. Предлагаются примеры заимствования отдельной терминологии из зарубежного законодательства в российское уголовное право. Дается квалификация отдельных действий в себе киберпреступность в соответствии с новыми понятиями уголовного права. С целью решения поставленной задачи в представленном научном исследовании применялись сравнительно-правовой и системный методы научного познания, позволившие рассмотреть проблему нового терминологического использования. Основным выводом проведенного исследования является то, что совершенствование терминологии и понятийного аппарата в системе национальной безопасности будет способствовать развитию ее нормативно-правового обеспечения, а также совершенствованию уголовного законодательства Российской Федерации в данной сфере, что в свою очередь будет способствовать предотвращению информационных войн и информационного терроризма.*

Ключевые слова: *Информационная безопасность, информационное пространство, информационная угроза, информационное преступление, информационный терроризм, информационная война, хакер, компьютерный вирус, уголовная ответственность, киберсфера.*

Abstract: *The subject of this research is the issue of forming a conceptual and terminological system within the sphere of safe handling of computer information within the criminal law aspect. Research is conducted on such concepts as cybernetics, information space, computer crime, cybercrime, information-technology terrorist act, information threat, information attack, etc. The author examines the examples of use of similar terminology within the foreign criminal legislation. Propositions are made on borrowing certain terminology from the foreign legislation and adopting it into the Russian criminal law. The main conclusion of the conducted research is the fact that improving terminology and conceptual apparatus within the system of national security would contribute to the development of its normative-legal functionality, as well as improving the criminal legislation of the Russian Federation within this sphere, which would in turn help prevent information warfare and information terrorism.*

Keywords: *Information warfare, information terrorism, information crime , information threat, information space, information security, hacker, computer virus, criminal responsibility, cybersphere.*

Важной теоретической составляющей любой социально значимой деятельности является наработка понятийно-терминологического аппарата, который обеспечивает надлежащий уровень отраслевой и общей коммуникации субъектов этой деятельности.

К вопросам, касающимся терминологии, связанной с информатикой, информатизацией, которая на протяжении последних 10 – 15 лет активно включается в юридическую лексику, обращались М.Г. Абрамова и А.В. Попов, И.Л. Бачило и П.У. Кузнецов, Ю. В. Волков и др. Ученые указывают, что использование сложных технических терминов в языке права и закона само по себе является сложной проблемой, поскольку нормы закона должны быть понятны и лицам, далеким от информационной сферы, что требует их соответствующего разъяснения и трактовки.

Рассматривая данную проблему, следует в первую очередь, обратить внимание на то, что в правовой

DOI: 10.7256/1811-9018.2015.4.14776
При цитировании этой статьи сноска на doi обязательна

терминологии России, в научном юридическом дискурсе широкое распространение получили термины киберпространство, киберпреступление, кибератака, кибероружие и другие, которые относятся к особо динамической и специфической сфере деятельности человека, связанной с обменом и обработкой электронных данных в глобальных информационно-коммуникационных сетях.

В тоже время, следует констатировать, что термины с приставкой «кибер» еще не получили сформированного общепризнанного значения ни на научном, ни на нормативно-правовом уровне и остаются предметом открытой дискуссии.

Несмотря на это, сфера, к которой относятся явления, обозначенные этими терминами (киберсфера) благодаря их общественной значимости, в настоящее время стала объектом внимания на государственном и международном уровнях, а также объектом актуальных научных исследований.

С целью адекватного содержательного наполнения понятийно-терминологического аппарата киберсферы целесообразно, во-первых, обратиться к источнику возникновения приставки «кибер» – кибернетики и генезиса ее значения, во-вторых, установить группу терминов, которые будут иметь ключевое значение для всего терминологического аппарата.

Впервые термин «кибернетика» был введен в оборот древнегреческим философом Платоном для обозначения искусства кормчего (в переводе с греческого кибернетика – искусство управления). В 1834 г. французский ученый Андре Мари Ампер использовал этот термин для обозначения несуществующей еще в то время науки об управлении обществом. Официальной датой рождения кибернетики как отдельной науки считается год опубликования книги Норберта Винера «Кибернетика» (1947), в которой он определил кибернетику как науку об управлении и связях в живой природе и в технических системах [1].

В современном понимании кибернетика – это наука об управлении, связи и переработке информации. Объектом исследования современной кибернетики являются кибернетические системы, рассматриваемые абстрактно (безотносительно к их реальной природе), что позволяет проводить исследования технических, биологических, социальных систем общими методами.

Исследование словарей [2] и научных статей [3], посвященных проблемам кибернетики как исходного термина, определяющего различные киберреалии, позволяют автору данной статьи констатировать, что с точки зрения лингвистики «кибер» – это приставка, обозначающая отношение явления, реалии либо предмета к робототехнике, искусственному интеллекту, виртуальному миру и т.д.

Отсутствие конкретики, как представляется автору статьи, не дает оснований для использования данного термина в качестве исходного для характеристики уголовно-правовых явлений, поскольку его «виртуальность», в определенном смысле, переводит проблемы безопасного обращения компьютерной информации в сферу правовой абстракции, в силу чего данное понятие трудно поддается правовой конкретизации, даже в том случае, если мы обратимся к широкому кругу методов конкретизации понятий и терминов, входящих в методологические основы уголовного права. Именно абстрактность приставки «кибер», отсутствие ее абсолютного лексического аналога в русском языке, излишне усложняет терминологическое поле информационной безопасности, вносит в данную сферу элементы философского дискурса, неуместного в данном случае, поскольку данная терминология активно входит в лексику нормативно-правового поля, в принципе, не совместимой с абстракцией, двусмысленностью либо неопределенностью.

С точки зрения уголовно-правовой семантики, представляется целесообразным отойти от «кибер» – терминологии, перейти к традиционной русской, к терминам, известным национальному уголовному и информационному праву, т.е. все известные явления, реалии, процессы, описываемые с помощью приставки «кибер», трансформировать в аналогичные явления, описываемые с помощью понятия «информация», «компьютер», иначе говоря, по нашему убеждению, понятие «киберсфера» может без всяких потерь быть заменено понятием «информационная сфера», понятием «киберпреступность» – компьютерная преступность, кибер-система – информационная система и т. д.

Как представляется автору этой статьи, информационная система является основой терминологического аппарата, касающегося проблем безопасного обращения компьютерной информации. С методологической точки зрения ее можно представить в виде совокупности взаимосвязанных объектов – элементов системы, которые способны запоминать, обрабатывать информацию и обмениваться ею с другими элементами и внешним миром. Система может изменять структуру в результате возникновения новых элементов, исчезновения старых, а также изменения связей между элементами. Примерами таких искусственных систем является компьютер, мобильный телефон, цифровая видеокамера и т.д. Компьютер рассматривается как

DOI: 10.7256/1811-9018.2015.4.14776
При цитировании этой статьи сноска на doi обязательна

универсальный преобразователь информации, способный, запоминая структуру другой информационной системы, выполнять ее функции как преобразователя информации. Именно эти качества делают его наиболее функциональным инструментом и основным техническим средством создания, распространения и использования информации.

Фундаментальное место в терминологическом аппарате информационной сферы целесообразно отдать термину «информационный простор», что означает среду, которая создает интегративную основу для всех информационных явлений. И хотя закрепление этого термина на законодательном уровне не представляется обязательным, установление герменевтических особенностей информационного пространства будет способствовать адекватному содержательному наполнению всего понятийно-терминологического аппарата информационной сферы.

Основываясь на современном понимании кибернетики, информационное пространство можно рассматривать как сложную систему, которая неразрывно сочетает в себе характеристики социальных и технических кибернетических систем [4]. Самые существенные из этих характеристик соответствуют чертам современных глобальных информационно-коммуникационных сетей (систем): широкие возможности управления, связи и объемы обработки информации; реализация с помощью компьютерных систем; тесная связь технологий информационного пространства с интеллектом человека (технологии выступают продолжением разума на пути эффективного достижения цели); присутствие как детерминированных закономерностей, так и синергетических, и случайных процессов; необъятность пределов развития и трансформации .

Учитывая те или иные из указанных характеристик, можно сформировать широкое и узкое понимание информационного пространства.

В широком смысле информационное пространство совпадает со сферой использования компьютеров, автоматизированных систем, компьютерных сетей и сетей электросвязи. На общенаучном уровне такой подход может быть вполне допустимым. Однако переход в сферу правового регулирования привносит свой специфический акцент, поскольку право – универсальный социальный регулятор, предметом его регулирования являются общественные отношения (поведение субъектов).

Выделение сферы общественных отношений, связанной с информационным пространством или информационной сферой в качестве предмета правового регулирования, поднимает новые проблемы, которым до этого времени не уделялось достаточного внимания. Во-первых, важным является разграничение новых для сферы правового регулирования видов поведения субъекта, относящихся к информационному пространству и уже регламентированного правовыми нормами поведения, что касается компьютерных систем как объектов материального мира. Во-вторых, не менее важным является осознание содержания поведения в информационном пространстве и его внешнего выражения.

Очевидно, что в рамках широкого понимания информационного пространства, решение этих проблем усложняется, поскольку действия, связанные с созданием, модификацией, уничтожением материальных компонентов компьютерных систем и сетей, а также физическим вмешательством в их функционирование, могут быть отнесены к действиям в информационном пространстве, при этом, не имея непосредственной связи с использованием его технологических возможностей.

Нерешенность данной проблемы прослеживается и в Европейской Конвенции о киберпреступности, которая не предусматривает ограничения способов и целей противоправных действий в отношении компьютерных систем, сетей и данных, относя все их проявления к компьютерным преступлениям, т.е. преступлениям, которые так или иначе связаны с преступной деятельностью в информационном пространстве [5].

Одним из путей решения обозначенных проблем, а также проблемы гармонизации терминологии может стать более узкое понимание информационного пространства.

В узком смысле современные исследователи отождествляют информационное пространство с совокупностью информационных ресурсов (фактов, сведений, реалий), находящихся в свободном (открытом) либо закрытом доступе, доступных для обработки с помощью средств компьютерной техники.

Соответственно, в таком понимании, информационное пространство можно определить как созданную с помощью компьютера информационную реальность, в структуре которой находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символьном или любом другом виде, находящиеся в процессе движения по локальным и глобальным компьютерным сетям либо сведения, хранящиеся в памяти любого физического или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи [6].

Другими словами, информационное пространство оказывается в единстве информационных ресурсов, представленных в виде электронных компьютерных

DOI: 10.7256/1811-9018.2015.4.14776
При цитировании этой статьи сноска на doi обязательна

данных и совокупности технологий, обеспечивающих возможности их обмена и преобразования. Согласно этому подходу, к действиям в информационном пространстве необходимо относить только те деяния, которые связаны с непосредственным использованием технологических возможностей преобразователей информации (компьютеров, мобильных телефонов) в информационном пространстве, независимо от последствий, которые они вызывают.

Таким образом, информационное пространство – это сформированная информационно-коммуникационными системами реальность, в которой протекают процессы преобразования (создания, хранения, обмена, обработки и уничтожения) информации, представленной в виде электронных компьютерных данных. Инициирование этих процессов и управление ими целесообразно рассматривать как внешнее выражение поведения субъекта в информационном пространстве, а само информационное пространство обязательно должно рассматриваться в качестве сферы практической деятельности субъекта, правообладателя, создателя, пользователя информации.

Особенно актуальной для правовой системы России представляется проблема формирования и содержательного наполнения комплекса терминов, связанных с противоправными деяниями в информационной сфере.

Отметим, что российскими учеными активно используются термины «компьютерное преступление», «преступления в сфере компьютерной информации», «преступления в сфере использования компьютеров», «преступления в сфере использования информационных технологий». Большинство авторов, анализируя компьютерную преступность, относят к ней преступления в сфере использования компьютеров, систем и компьютерных сетей, сетей электросвязи и определяют их как посягательство на отношения в сфере компьютерной обработки информации, права собственности физических и юридических лиц на информацию и доступ к ней. Очевидно, что в таком понимании понятие компьютерного преступления является одним из сегментов понятийного аппарата, касающегося противоправных деяний в информационной сфере.

Как представляется, сущность противоправных деяний в информационной сфере отражает понятие компьютерного преступления, которое, по мнению специалистов, может определяться как виновное противоправное вмешательство в работу компьютера, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные деяния, совершенные с помощью компьютеров, компьютерных сетей и программ [6].

Отметим, что зарубежными специалистами понятие преступление, совершенное в информационном пространстве, охватывает любые противоправные деяния, осуществляемые с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети [7,8,9].

Общий перечень этих деяний обозначен Конвенцией о киберпреступности. К ним относятся: незаконный доступ к компьютерной системе, нелегальный перехват данных, вмешательство в данные, вмешательство в систему, злоупотребление устройствами, подделка и мошенничество, связанные с компьютерами; правонарушения, связанные с детской порнографией; правонарушения, связанные с нарушением авторских и смежных прав [5].

Следует подчеркнуть, что как Конвенцией о киберпреступности, так и большинством научных трудов в этой сфере, противоправные деяния рассматриваются безотносительно степени общественной опасности (вреда), но требуется установление на уровне национальных законодательств уголовной ответственности за эти деяния.

Одновременно, ст. 14 УК Российской Федерации определяет, что не является преступлением действие (бездействие), хотя формально и содержащее признаки какого-либо деяния, предусмотренного настоящим Кодексом, но в силу малозначительности не представляющее общественной опасности [10].

Сказанное свидетельствует о необходимости интерпретации противоправных деяний в информационной сфере сквозь призму социальной опасности деяния, выделяя две группы правонарушений: преступления – наиболее общественно опасные деяния, определенные УК Российской Федерации и малозначительные деяния, которые не могут быть отнесены к категории преступлений, поскольку не представляют существенной общественной опасности, иначе говоря – проступки или правонарушения, уголовная ответственность за которые не наступает.

В этой связи целесообразным представляется введение родового понятия, касающегося уголовно ненаказуемых неправомерных деяний в информационной сфере – понятия «компьютерное правонарушение», что обеспечит дифференциацию уголовной ответственности, индивидуализацию наказания.

Данное противоправное действие может быть определено как общественно опасное виновное деяние, которое осуществляется с использованием технологий

DOI: 10.7256/1811-9018.2015.4.14776
При цитировании этой статьи сноска на doi обязательна

преобразования (создания, хранения, обмена, обработки и уничтожения) информации, представленной в виде цифровых данных, и влечет за собой юридическую ответственность. Компьютерное правонарушение имеет все общие признаки правонарушений, выделяемых в теории права, и отличается лишь факультативной частью юридического состава, в котором информационное пространство выступает как средство совершения правонарушения.

Соответственно, к компьютерным преступлениям следует отнести наиболее опасные компьютерные правонарушения, за которые устанавливается уголовная ответственность, а к компьютерным проступкам – все остальные информационные правонарушения, которые не несут существенной общественной опасности и за которые предусматривается юридическая ответственность других видов, прежде всего, гражданско-правовая и административная.

Учитывая современные тенденции понимания информационной безопасности, компьютерные правонарушения можно рассматривать в узком и широком смысле. В узком, – это противоправные деяния, которые привели к нарушению конфиденциальности, целостности, авторства и доступности информации в информационно-телекоммуникационных системах в рамках их технологических функций. В широком смысле к компьютерным правонарушениям дополнительно можно отнести противоправные деяния, которые привели к реализации деструктивных информационно-психологических воздействий на сознание, психологическое и психическое состояние людей, совершенные с использованием возможностей современных информационно-телекоммуникационных систем.

Следует отметить, что технологическая составляющая всех компьютерных правонарушений является одинаковой – это использование технических недостатков механизмов безопасности современных информационно-коммуникационных систем, методов социальной инженерии и современных технологических возможностей воздействия на целевую аудиторию через информационное пространство, что делает его несравненно действенным средством достижения различных преступных целей. Кроме того, целесообразно учитывать технологические возможности построения скрытых каналов связи и управления в информационно-телекоммуникационных системах, которые могут быть использованы для организации противоправной деятельности, в том числе разведывательно-подрывного и террористического характера.

Именно поэтому в наше время наибольшего внимания требуют преступления против основ национальной безопасности, которые благодаря эффективности информационного пространства как средства осуществления, могут приобрести угрожающие масштабы. К ним, в первую очередь, относятся терроризм, шпионаж, государственная измена, публичные призывы к насильственному изменению или свержению конституционного строя или к захвату государственной власти, а также дискредитация органов власти и государства на международной арене. Самым опасным из них является современное проявление терроризма – информационный терроризм.

В общем понимании информационный терроризм представляется как общественно опасная деятельность, которая заключается в сознательном, целенаправленном устрашении населения и органов власти и осуществляется с использованием информационно-телекоммуникационных систем с целью достижения преступных целей.

Терроризм имеет много проявлений и составляющих, однако квинтэссенцией террористической деятельности является террористический акт, который во взаимосвязи с информационным пространством целесообразно выделить в качестве отдельного понятия – «информационно-технологический террористический акт», который можно определить как вмешательство в работу компонентов информационно-телекоммуникационных систем и их программного обеспечения или как несанкционированная модификация компьютерных данных, что вызывает дезорганизацию работы критически важных элементов хозяйственной, военной инфраструктуры, а также системы государственного управления и создает опасность для жизни или здоровья человека, влечет за собой значительный имущественный ущерб или наступление других тяжких последствий.

Современный период развития Российской Федерации отмечен постепенным формированием комплексных подходов к национальной безопасности, среди которых обеспечение информационной безопасности занимает одно из ведущих мест и определяется как состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления незапрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность [11].

DOI: 10.7256/1811-9018.2015.4.14776
При цитировании этой статьи сноска на doi обязательна

В контексте нормативно-правового понимания национальной и информационной безопасности, информационная безопасность может определяться как защищенность жизненно важных интересов человека и гражданина, общества и государства, при которой обеспечивается стабильное развитие общества, своевременное выявление, предотвращение и нейтрализация реальных и потенциальных угроз национальным интересам в сфере функционирования информационно-телекоммуникационных систем. В технологическом контексте информационная безопасность – это процесс защиты информационного пространства от реальных и потенциальных информационных угроз. На философско-социологическом уровне осмысления информационную безопасность можно интерпретировать через совокупность условий функционирования субъекта в информационном пространстве, обеспечивающих его оптимальный информационный комфорт.

Как представляется автору данной статьи, в настоящее время, кроме указанных выше терминологических уточнений, осмысления и конкретизации также требуют и такие понятия как «информационная угроза», «информационная защита», «информационная война», «информационная атака», которые активно входят в отечественный правовой дискурс под воздействием сложных политических процессов, направленных, в том числе, и на подавление информационного суверенитета России.

По мнению автора статьи, информационная угроза представляет собой дестабилизирующий фактор, отрицательно влияющий на объект, возникает как следствие использования технологических возможностей программного обеспечения, компьютеров, иных преобразователей информации в информационном пространстве. К информационным угрозам относятся угрозы по поводу нарушения конфиденциальности, целостности, авторства, доступности информации, также угрозы деструктивных информационно-психологических воздействий на сознание, психологическое и психическое состояние человека.

Информационная защита, в свою очередь, может быть определена как комплекс мер правового, организационного, экономического, технологического, идеологического характера, направленных на обеспечение надлежащего уровня нивелирования информационных угроз.

Информационная война в общем понимании – это активное противостояние между субъектами, которое предполагает применение наступательных (оборонительных) действий в информационном пространстве с целью нанесения (противодействия нанесению) вреда любого характера. На международном уровне информационная война – это способ разрешения противоречий между государствами и нациями средствами деструктивного влияния через информационное пространство.

В свою очередь, информационное оружие представляет собой совокупность информационно-телекоммуникационных технологий, которые используются для достижения преступных целей и нанесения ущерба через информационное пространство.

Информационная атака представляет собой одну из самых масштабных информационных угроз современности и может рассматриваться и как самостоятельное явление, и как квинтэссенция ведения информационной войны или осуществления террористической деятельности в информационном пространстве. В таком контексте просматриваются параллели между информационной атакой и информационно-террористическим актом, а поскольку эти понятия полностью не совпадают, то возникает необходимость наработки правовой дефиниции информационной атаки как преступления.

Информационная атака в общем понимании – это использование технических недостатков механизмов безопасности современного информационного пространства с целью дезорганизации работы его элементов. С уголовно-правовой точки зрения информационная атака должна выражаться в форме действия, которое заключается во вмешательстве в работу компонентов информационно-телекоммуникационных систем и их программного обеспечения или несанкционированной модификации компьютерных данных, которая осуществляется через информационно-телекоммуникационные сети с целью дезорганизации работы их элементов.

Следует отметить, что новейшие политические тенденции, реальность возникновения новой «холодной войны», что является следствием политической близорукости отдельных государств, формируют политическую реальность, схожую по своему содержанию с реальностью, описываемую термином «холодная война». Не обращаясь к его трактовке, лишь отметим, что для данного политического процесса характерно и усиление информационного противостояния, которое может, в конечном итоге, трансформироваться в информационную войну, в процессе которой, наряду с развертыванием активной антироссийской пропаганды, могут возникнуть угрозы террористической деятельности в информационном пространстве, развиваться и иные формы информационного противостояния, напрямую касающиеся проблем безопасности России [12,13,14].

В этой связи актуальным представляется также рассмотрение таких понятий как информационная инфраструктура государства, которая, по нашему

DOI: 10.7256/1811-9018.2015.4.14776
При цитировании этой статьи сноска на doi обязательна

мнению, может быть определена как совокупность информационно-телекоммуникационных систем и сетей (вычислительных средств, каналов обмена данными, систем хранения данных, средств коммутации и управления информационными потоками), обеспечивающих функционирование механизма государства. Причем, в широком понимании, к информационной инфраструктуре государства необходимо отнести также и организационные структуры, и нормативно-правовые механизмы, обеспечивающие надлежащее функционирование информационно-телекоммуникационных систем и сетей.

Подводя итог данной статьи, следует указать на то, что информационная сфера (сфера обмена и обработки информации, которая представлена в виде электронных компьютерных данных), играет все большее значение в процессах развития российского общества, а криминальные проявления в этой сфере приобретают угрожающие масштабы, что предопределяет необходимость охвата ее регулятивными и охранительными функциями права, а также повышает внимание к информационной безопасности как к отдельной составляющей национальной безопасности России. В таких условиях важным является системный подход к формированию понятийно-терминологического аппарата безопасного обращения компьютерной информации, который обеспечит ее адекватное содержательное наполнение, соответствие требованиям, предъявляемым к правовой терминологии, а также гармонизацию с традициями русского уголовного права и терминологией действующего уголовного законодательства Российской Федерации.

Библиография:

1. Сергеев А.П. Право интеллектуальной собственности в Российской Федерации: учеб. 2-е изд., перераб. и доп. – М.: Велби, Издательство Проспект, 2005. 883 с.
2. Большой толковый словарь русского языка / сост. С.А. Кузнецов; 1-е изд. – СПб.: Норинт, 2000. 1536 с.
3. Нестеров А.В. Существует ли информационная безопасность, или некоторые аспекты законопроекта технического регламента «О безопасности информационных технологий» // «Правовые вопросы связи», 2007, № 1. С. 31-34.
4. Абрамова М.Г., Попов А.В. К вопросу о содержании понятий «информация», «информационные технологии» и «информационное право» // Образование и право. 2012. № 3. С. 192-195
5. Конвенция о киберпреступности от 23.11.2001 [Электронный ресурс]. – Режим доступа: http://stra.teg.ru/library/national/34/evro/konv_kiber
6. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дисс. … канд. юрид. наук. – Владивосток, 2005. 235 с.
7. Loundy David J. Information Systems Law and Operator Liability Revisited, Murdoch University E-Law Journal, vol. 1, 3, September 1994.
8. McMahon John. Practical DECnet Security, Digital Systems Journal, vol. 14, November 1992.
9. Melford Robert J. Network security; computer networks, Internal Auditor, institute of Internal Auditors, vol. 50, February 1993.
10. Уголовный Кодекс РФ от 13.06.96 № 63-ФЗ [Электронный ресурс]. – Режим доступа: http://zakonbase.ru/ugolovnyj-kodeks
11. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895) [Электронный ресурс]. – Режим доступа: http://base.garant.ru/182535/#ixzz3KjcbnX5U
12. Бачило И. Л., Кузнецов П. У. Правовое обустройство информационной действительности: проблемы и перспективы // Российский юридический журнал, 2008, № 5
13. Волков Ю. В. Термин «информация» в контексте законодательства // Юрислингвистика. 2011. № 11. С. 424-426.
14. Федотов М. А. К вопросу о концептуальных основах информационного права как права киберпространства // Вопросы правоведения. 2011. № 3. С. 71-98.

References (transliterated):

1. Sergeev A.P. Pravo intellektual'noi sobstvennosti v Rossiiskoi Federatsii: ucheb. 2-e izd., pererab. i dop. – M.: Velbi, Izdatel'stvo Prospekt, 2005. 883 s.
2. Nesterov A.B. Sushchestvuet li informatsionnaya bezopasnost', ili nekotorye aspekty zakonoproekta tekhnicheskogo reglamenta «O bezopasnosti informatsionnykh tekhnologii» // «Pravovye voprosy svyazi», 2007, № 1. S. 31-34.
3. Abramova M.G., Popov A.V. K voprosu o soderzhanii ponyatii «informatsiya», «informatsionnye tekhnologii» i «informatsionnoe pravo» // Obrazovanie i pravo. 2012. № 3. S. 192-195
4. Tropina T.L. Kiberprestupnost': ponyatie, sostoyanie, ugolovno-pravovye mery bor'by: diss. … kand. yurid. nauk. – Vladivostok, 2005. 235 s.
5. Loundy David J. Information Systems Law and Operator Liability Revisited, Murdoch University E-Law Journal, vol. 1, 3, September 1994.

DOI: 10.7256/1811-9018.2015.4.14776
При цитировании этой статьи сноска на doi обязательна

6. McMahon John. Practical DECnet Security, Digital Systems Journal, vol. 14, November 1992.
7. Melford Robert J. Network security; computer networks, Internal Auditor, institute of Internal Auditors, vol. 50, February 1993.
8. Bachilo I. L., Kuznetsov P. U. Pravovoe obustroistvo informatsionnoi deistvitel'nosti: problemy i perspektivy // Rossiiskii yuridicheskii zhurnal, 2008, № 5
9. Volkov Yu. V. Termin «informatsiya» v kontekste zakonodatel'stva // Yurislingvistika. 2011. № 11. S. 424-426.
10. Fedotov M. A. K voprosu o kontseptual'nykh osnovakh informatsionnogo prava kak prava kiberprostranstva // Voprosy pravovedeniya. 2011. № 3. S. 71-98.