

ИССЛЕДОВАНИЯ В ОБЛАСТИ ГУМАНИТАРНЫХ НАУК

ТЕНДЕНЦИИ ФОРМИРОВАНИЯ РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КАСАТКИН В. П.,

д.и.н., профессор кафедры

«Теории и истории государства и права»

Белгородского Государственного Университета» (БелГУ)

ВАРФОЛОМЕЕВ М. А.,

аспирант кафедры

«Теории и истории государства и права»

Белгородского Государственного Университета» (БелГУ)

e-mail: max-varfolomeev@yandex.ru

В статье 19 Всеобщей Декларации прав человека, утвержденной и провозглашенной Генеральной ассамблеей ООН 10 декабря 1948 года, говорится: "каждый имеет право искать, получать, распространять информацию...". Развитие указанной нормы нашло отражение в статье 10 Европейской Конвенции о защите прав человека и основных свобод», (вступила в силу 3 сентября 1953 года), где указано, что «свободы получения и распространения информации реализуются без какого-либо вмешательства со стороны государственных органов». В статье 19 Международного пакта о гражданских и политических правах», (вступил в силу 23 марта 1976 года) уточняется, что эти свободы относятся к разного рода информации, идеям и способам их распространения.¹ Фундамент для дальнейшего развития законодательства был заложен Декларацией прав человека и гражданина, принятой 22 ноября 1991 года Верховным Советом РСФСР. В указанном документе впервые на уровне конституционных норм появился термин "информация". В соответствии со статьей 13 Декларации "каждый имеет право искать, получать и свободно распространять информацию..."².

В интересах обеспечения информационной безопасности в России, «правовой защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу».³ Правовой режим информации представляет собой нормативно установленные правила, определяющие степень открытости, порядок документирования, доступа, хранения, распространения и защиты

информации, а также исключительные права на информацию.

Понятие и термин "информационные отношения" получил законодательное закрепление.⁴ Под ними понимаются отношения по поводу сбора, накопления, хранения и использования информации. Представляется, что это определение является неполным, так как не охватывает все информационные процессы, по поводу которых и возникают информационные правоотношения. Содержание информационных процессов представлено в Федеральном законе "Об участии в международном информационном обмене"⁵ позволяет дать более полное определение понятия информационных правоотношений.

Анализ действующего законодательства в рассматриваемой сфере позволяет утверждать о том, что информационное законодательство, должно состоять из базового закона и набора нормативных правовых актов, формируемых в его развитии, так как регулировать всю совокупность отношений в области информационной безопасности одним законом нецелесообразно (в этом случае оно окажется громоздким, перегруженным частными нормами).

Таким образом, при формировании законодательства в сфере информационной безопасности необходимо учитывать не только его принципы, но и принципы всего информационного законодательства. В качестве направления формирования и развития рассматриваемого законодательства можно выделить систематизацию нормативных правовых актов в этой сфере.

Необходимость систематизации нормативных правовых актов в сфере информационной безопасности обусловлена определением информационного

¹ Всеобщая Декларация прав человека, утв. Генеральной ассамблеей ООН 10 декабря 1948 г. Европейская Конвенция о защите прав человека и основных свобод, от 3. 09. 1953г. Международный пакт о гражданских и политических правах, от 23. 09. 1976 г. Сборник нормативных документов. - М.: Мир безопасности, 1999. 800 с.

² См. там же.

³ ФЗ РФ «О безопасности», от 5 марта 1992 г. - Российская газета, от 6.05.92г.

⁴ ФЗ РФ № 24 «Об информации, информатизации и защите информации» от 20 февраля 1995 г. - Российская газета от 22.04.95г.

⁵ ФЗ РФ № 86 «Об участии в международном информационном обмене» от 4 июля 1996 г. - Российская газета от 11.08.96г.

законодательства в системе российского законодательства и круга информационных правоотношений, подлежащих правовому регулированию.

Исходя из рассмотренного выше, можно утверждать, что: в основу классификации информационных технологий должен быть положен определенный набор классов комплексной защищенности информационно-вычислительных систем, учитывающих характеристики уязвимости, ценности и секретности информации, функциональные особенности конкретных прикладных систем. Необходима разработка и введение в действие единой государственной системы нормативных документов, например, государственных стандартов, устанавливающих применительно к указанным классам соответствующие нормы защищенности. К ним относятся: требования по применению защищенных средств вычислительной техники (применение сертифицированных средств вычислительной техники не ниже определенного класса защищенности), требования и рекомендации по составу, функциональным и качественным характеристикам используемых и вновь разрабатываемых технических средств защиты, а также рекомендации по применению необходимых административных и организационных мер защиты.

Кроме введения норм защищенности следует также создать систему сертификации средств защиты информации, поступающих на рынок средств вычислительной техники, и ввести систему лицензирования работ в области информационной безопасности. Можно также рассчитывать на определенное позитивное влияние процессов международной и отечественной стандартизации в области информационной безопасности, на разработку и производство средств защиты и защищенных средств вычислительной техники, так как в настоящее время наблюдается определенный "прорыв", связанный с активизацией усилий различных международных организаций в этом направлении. Политика организаций, осуществляющих страхование автоматизированных систем, информационных ресурсов и компьютерной информации, также может способствовать расширению практического внедрения современных средств защиты информации. Требование страховых компаний к своим клиентам по обеспечению надлежащего уровня безопасности информации за счет применения сертифицированных систем защиты представляется вполне естественным и справедливым.

Гражданский кодекс Российской Федерации определяет информацию как один из видов объектов гражданских прав.⁶ В связи с возрастающим хранением и использованием информации в электронном виде чаще используется понятие "электронный документ". Одним из распространенных способов подтверждения подлинности такого документа является электронная цифровая подпись. В пункте 2 статьи 160 Гражданского кодекса РФ впервые было закреплено использование электронной цифровой подписи при совершении сделок лишь в случаях, предусмотренных соответствующими законами. В

этом случае принятие закона "Об электронном документе" весьма актуально.

Законодательство об интеллектуальной собственности в настоящее время также нуждается в совершенствовании. Так, правовая охрана в соответствии с Патентным законом не предоставляется секретным изобретениям, полезным моделям, промышленным образцам.⁷ Порядок обращения с такими разработками должен регулироваться специальным законом. Более целесообразным может быть внесение дополнений в Закон РФ "О государственной тайне".

Государство не только должно защищать информацию и права граждан на доступ к информации, но и создавать условия для защиты самого человека и общества от вредоносного вида определенной информации.⁸ Например, к такой информации можно отнести:

- информацию, возбуждающую социальную, расовую, национальную вражду;
- посягательство на честь, доброе имя и деловую репутацию людей;
- информацию, оказывающую деструктивное воздействие на психику людей.

Актуальным и по-прежнему неурегулированным остается вопрос, связанный со всемирно известной сетью Интернет, которая в настоящее время состоит из огромного множества компьютеров, объединенных между собой средствами телекоммуникаций. Бесспорно, она открыла новые возможности в области информационного обмена. Вместе с тем есть ряд отрицательных моментов: прежде всего сеть Интернет не находится в собственности какого-либо физического лица, организации, государства или его органов и как следствие - отсутствие государственного регулирования, цензуры, иных форм контроля за информацией, циркулирующей в сети. Такое положение также открывает новые и неограниченные возможности для ведения незаконной деятельности.

Стремление стран к доминирующему положению, связанному с владением сети Интернет, как правило, несет опасность циркуляции недоброкачественной информации. Опасность распространения "вредной и разрушающей" информации в сети Интернет для информационно-психологического воздействия на людей очевидна и не требует комментариев.

Необходимость создания комитета или совета по проблемам Интернета в целях координации и принятия решений правового регулирования рассматриваемой проблемы очевидна.

Одним из эффективных путей укрепления правопорядка является своевременное, полное и достоверное информационное обеспечение деятельности правоохранительных органов. Развитие системы информационного обеспечения определяется через ключевое направление. Оно выражается через единые методические, информационные,

⁷ ФЗ РФ № III. 3517-1. «Патентный закон Российской Федерации» от 23 сентября 1993г. Российская газета от 3.10.93г.

⁸ Концепция правовой информатизации России. Принята Указом Президента Российской Федерации 23 июня 1993 г.

⁶ Гражданский кодекс Российской Федерации 2005г. – М.: Кодекс, 2005. 872 с.

организационно-правовые и программно-технические решения, выработанные на основе системного подхода.

Определенная роль отводится компонентам информационного обеспечения - технологии и интегрированным банкам данных. Уделяется внимание обеспечению единства информационной поддержки основных стадий уголовно-процессуальной деятельности путем пересмотра функциональных возможностей имеющихся оперативно-справочных, розыскных и криминалистических учетов и создания информационно-вычислительной системы ОВД России.

В этой связи предполагается ввести три группы нормативно-правовых документов по информационному обеспечению, а именно:

- а) отраслевые, общего пользования;
- б) отраслевые, по линиям служб;
- в) нормативно-правовая документация местного уровня управления по локальным, прикладным проблемам информационного обеспечения территориальных органов внутренних дел.

Таким образом, существует необходимость дальнейшего развития правовой базы органов внутренних дел в сфере обеспечения информационной безопасности. Такое развитие должно осуществляться в рамках соблюдения основного принципа уважения прав и свобод человека и гражданина, информационного обеспечения деятельности органов внутренних дел, обеспечения защиты информационных систем и циркулирующей в них информации от несанкционированного доступа.

Подводя итоги рассмотренных вопросов, можно сделать следующие выводы:

1. Формирование законодательства об информа-

ции и информационной безопасности соответствует задаче создания национальной, правовой информационной системы РФ. Для определения основных направлений формирования законодательства в информационной сфере необходимо уточнить само понятие "информационное законодательство".

2. При формировании структуры законодательства в информационной сфере следует учитывать два момента: принципы построения и упорядочение существующих нормативных актов по информационной безопасности, ориентированных, прежде всего, на обеспечение прав и свобод личности.

Проведенный анализ позволяет выделить следующие принципы:

- равенства субъектов информационных отношений;
- информационной безопасности и защиты информации;
- свободы информации с установлением ограничений доступа к отдельным видам информации и информационных ресурсов.

3. В качестве основных направлений формирования и развития рассматриваемого законодательства можно выделить следующие:

- первоочередная реализация конституционных прав граждан в информационной сфере;
- обеспечение приоритета федерального законодательства и совершенствование на этой основе законодательства субъектов федерации в информационной сфере;
- реализация государственной политики по принятию необходимых поправок в существующие законы, устранение пробелов в информационном законодательстве.

ИЗМЕНЕНИЕ ПОЛНОМОЧИЙ ПРЕЗИДЕНТА УКРАИНЫ В ПРОЦЕССЕ ПРОВЕДЕНИЯ КОНСТИТУЦИОННОЙ РЕФОРМЫ

ОЛЕЙНИК Н. Н.,
д.и.н.,

*профессор кафедры «Украиноведения»
Белгородского Государственного Университета;*

КУЗНЕЦОВ И. В.,
*аспирант кафедры Украиноведения
Белгородского Государственного Университета
e-mail: abenfica62@yandex.ru*

Выборы президента Украины состоявшиеся в октябре – декабре 2004 года и носившие затяжной, и поистине драматический характер, принесли не только победу Виктору Ющенко и тем политическим силам, которые его поддерживали, но и значительные изменения в Конституцию Украины.

Эти нововведения, непосредственно затрагивающие полномочия президента были закреплены в конституционном законе Украины "О внесении изменений в Конституцию Украины" принятого Верховной Радой 8 декабря 2004 года. Эти изменения и дополнения были внесены в следующие статьи: 76,

78, 81-83, 85, 87, 88, 89, 90, 93, 98, 106, 112-115, 116, 120, 121 Основного Закона Украины.

По мнению Председателя Верховной Рады Украины Владимира Литвина «принятый конституционный закон "О внесении изменений в Конституцию Украины" открыл реальную перспективу построения нового механизма управления государством»¹.

Необходимо отметить одно важное на наш взгляд обстоятельство, все перечисленные статьи, касающиеся полномочий президента, довольно существенно

¹ Голос Украины №238 от 16.12.2004.