

Информационная безопасность

ЗАКУПЕНЬ Татьяна Васильевна - доктор юридических наук, профессор кафедры правового обеспечения рыночной экономики Российской академии государственной службы при Президенте РФ

тел.: (495) 725-89-07

e-mail: zak1955@mail.ru

ПОНЯТИЕ И СУЩНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЕЕ МЕСТО В СИСТЕМЕ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Во всех составляющих национальной безопасности – политической, экономической, военной, правоохранительной, экологической и др. - вес информационных факторов непрерывно растет. Качество информации, ее достоверность, своевременность и полнота определяют не только добротность решений, принимаемых органами власти и управления. Информационно-психологические воздействия, реализуемые через средства массовой информации, могут создать атмосферу напряженности и политической нестабильности в обществе, спровоцировать социальные, национальные, религиозные конфликты и массовые беспорядки, привести к разрушительным последствиям для демократического развития страны. Незаконное использование, хищение или искажение деловой (банковской, коммерческой, статистической) информации неизбежно ведут к тяжелым экономическим потерям. Уровень развития информационных технологий, на которых основываются современные системы разведки, радиоэлектронной борьбы, управления войсками и высокоточным оружием, существенно предопределяет исход вооруженных конфликтов. Целенаправленные информационные воздействия могут создать труднопреодолимые препятствия на пути равноправного сотрудничества России с развитыми странами и дружественными государствами, подрывать международный авторитет страны. Нельзя также забывать, что информационные воздействия оказывают решающее влияние на процессы образования, формирования личности, ее духовного мира и могут вызвать неадекватное социальное или криминальное поведение групп людей и отдельных лиц, нанести физический, материальный и моральный ущерб гражданам. Именно поэтому национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, причем в ходе технического прогресса эта зависимость будет еще более возрастать.

Все сказанное выше заставляет с особым вниманием отнестись к угрозам национальной безопасности, осуществляемым в информационной сфере, глобальным проблемам обеспечения безопасности информации теми способами и методами, которые имеются в распоряжении права.

Для более четкого определения предметной области понятия «информационная безопасность» следует вначале охарактеризовать основы теории национальной безопасности, а также уяснить правовую природу категории «безопасность» в целом.

До последнего времени понятию «безопасность», методологическим проблемам безопасности как определенного социального явления уделялось мало внимания, что объяснялось закрытостью темы безопасности как монопольной сферы высшего политического руководства, рассматривающего это как понятие в основном и главным образом в связи с военными проблемами страны [1,2]. В общих энциклопедических изданиях, включая «Новый иллюстрированный энциклопедический словарь» (1999 год), это понятие отсутствует. В Большой советской энциклопедии раскрывается лишь понятие «безопасность международная», которое трактуется как состояние экономических, политических и других отношений между государствами, утверждающее мирное сосуществование государств на началах равноправия, национальную независимость и самостоятельность народов, а также их свободное развитие на демократической основе [3]. Этим понятие «безопасность» сводилось только к противодействию внешним опасностям и угрозам, утверждая тем самым официальную позицию того времени об отсутствии внутренних угроз для безопасности страны.

В. Даль указывал, что безопасность есть отсутствие опасности, сохранность, надежность [4]. По С. Ожегову безопасность – это «состояние, при котором не угрожает опасность, есть защита от опасности» [5].

Существует множество других определений безопасности: безопасность - свойство личности, общества и государства противодействовать угрозам опасности; безопасность - система мер, направленных на предотвращение опасности; безопасность - деятельность людей, общества, государства, мирового сообщества народов по выявлению (изучению), предупреждению, ослаблению, устранению (ликвидации) и отражению опасностей и угроз, способных погубить их, лишит фундаментальных материальных и духовных ценностей, нанести неприемлемый (недопустимый объективно и субъективно) ущерб, закрыть путь для выживания и развития [6,7].

В соответствии с Законом РФ «О безопасности» безопасность – это «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». В законе записано, что «жизненно важные интересы – это совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства». Исходя из этого, к основным объектам безопасности следует отнести:

- личность (ее права и свободы);
- общество (его материальные и духовные ценности);
- государство (его конституционный строй, суверенитет и территориальная целостность).

Субъектами обеспечения безопасности выступают:

- государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной власти;
- общественные и иные организации и объединения;
- граждане, которые в соответствии с законодательством обладают правами и обязанностями по участию в обеспечении безопасности Российской Федерации.

Главную роль при этом играет государство, которое в соответствии с действующим законодательством должно обеспечивать безопасность каждого гражданина, а также социальную и правовую защиту граждан и юридических лиц, оказывающих содействие в обеспечении безопасности в соответствии с законом [8].

Следует выделить несколько уровней обеспечения безопасности государства: а) личный - надежная защита личной и имущественной безопасности; б) на уровне организации гражданского общества – преодоление конфронтации в обществе, достижение и поддержание национального согласия, преодоление экономического кризиса и т.д.; в) на государственном уровне – неуклонное обеспечение суверенитета и территориальной целостности России; обеспечение социально-политической и экономической стабильности страны; совершенствование федеративного государственного устройства и т.п. Основным регулятором отношений в этих сферах должно стать право.

В Концепции национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 17 декабря 1997 г. № 1300, существенно дополнены и конкретизированы положения, ранее закрепленные в Законе Российской Федерации «О безопасности» [9]. В соответствии с Концепцией общенациональная безопасность реализуется в двух измерениях: общественном и государственном, и подразделяется на внутреннюю и внешнюю в зависимости от источников угроз, опасностей и рисков для жизненно важных интересов. Первоосновой безопасности является безопасность личности, что предопределяет безопасность гражданского общества и легитимность государства [10-11].

Основными задачами по обеспечению национальной безопасности Российской Федерации применительно к теме информационной безопасности являются:

- своевременное выявление и нейтрализация внешних и внутренних угроз национальной безопасности Российской Федерации;
- преодоление научно-технической и технологической зависимости Российской Федерации от внешних источников;
- обеспечение личной безопасности граждан Российской Федерации, их конституционных прав и свобод;
- обеспечение полноты и совершенствование законодательства Российской Федерации при обеспечении приоритета федерального законодательства;

- принятие эффективных мер по пресечению разведывательной и подрывной деятельности иностранных государств против Российской Федерации;
- разработка организационных и правовых механизмов защиты государственной целостности, единства правового пространства и национальных интересов России;
- выработка и реализация региональной политики, обеспечивающей оптимальный баланс федеральных и региональных интересов;
- совершенствование механизма предупреждения возникновения политических партий и общественных объединений, преследующих сепаратистские и антиконституционные цели, и пресечения их деятельности.

Представляется, что решение вышеназванных задач обеспечения национальной безопасности страны возможно лишь при создании целостной системы, включающей совокупность законодательных актов и созданных на их основе структур и механизмов взаимодействия по защите интересов субъектов правоотношений. Устойчивость системы должна основываться на общенациональном согласии.

Одной из основных составляющих системы обеспечения национальной безопасности является информационная безопасность, выступающая важным связующим звеном всех основных компонентов государственной политики в единое целое. При этом совершенно очевидно, что роль информационной безопасности и ее место в системе национальной безопасности страны становится все значительней. Это происходит в силу следующих причин:

- национальные интересы, угрозы им и обеспечение защиты от этих угроз во всех областях национальной безопасности выражаются, реализуются и осуществляются через информацию и информационную сферу;
- человек и его права, информация и информационные системы и права на них – это основные объекты не только информационной безопасности, но и основные элементы всех объектов безопасности во всех ее областях;
- решение задач национальной безопасности связано с использованием информационного подхода как основного научно-практического метода;
- проблема национальной безопасности имеет ярко выраженный информационный характер.

Вышеназванные обстоятельства, наряду с задачами построения гражданского общества в Российской Федерации как общества информационного, возрастанием роли информации, информационных ресурсов и технологий в развитии гражданского общества и государства в XXI веке выводят вопросы информационной безопасности на первый план в системе обеспечения национальной безопасности. Укрепление информационной безопасности названо в Концепции национальной безопасности Российской Федерации в числе важнейших долгосрочных задач. Роль информационной безопасности и ее место в системе национальной безопасности страны определяется также тем, что государственная информационная политика тесно взаимодействует с государственной политикой обеспечения национальной безопасности страны через систему информационной безопасности, где последняя выступает важным связующим звеном всех основных компонентов государственной политики в единое целое [12].

Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации представлена в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 9 сентября 2000 г. [13]. В ней *под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.*

Интересы личности в информационной сфере, а, значит, и правовое обеспечение ее информационной безопасности, состоят в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере состоят в создании условий для гармоничного развития российской информационной инфраструктуры, реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях укрепления конституционного строя, упрочения суверенитета и сохранения территориальной целостности России, для установления политической и социальной стабильности, экономического процветания, а также защите государственной тайны, безусловном исполнении законодательства и поддержании правопорядка, развитии международного сотрудничества на основе партнерства и соблюдения интересов России.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности. Исходя из анализа основных положений Доктрины, можно выделить четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Во-первых, это соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Во-вторых, это информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

И, наконец, четвертая составляющая представляет собой защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Следует отметить, что реализация указанных выше направлений в целом и любого из них в отдельности представляет собой достаточно сложную задачу, которую необходимо решать комплексно.

Во-первых, путем:

- повышения эффективности использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа России;

- усовершенствования системы формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;

- обеспечения конституционных прав и свобод человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;

- обеспечения конституционных прав и свобод человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;

- укрепления механизма правового регулирования отношений в области охраны интеллектуальной собственности, создания условий для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

- гарантирования свободы массовой информации и запрет цензуры;

- недопущения пропаганды и агитации, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;
- обеспечения запрета на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Во-вторых, путем:

- укрепления государственных средств массовой информации, расширения их возможностей по своевременному доведению достоверной информации до российских и иностранных граждан;
- интенсификации формирования открытых государственных информационных ресурсов, повышения эффективности их хозяйственного использования.

В-третьих, путем:

- развития и совершенствования инфраструктуры единого информационного пространства Российской Федерации;
- развития производства в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширения участия России в международной кооперации производителей этих средств и систем;
- обеспечения государственной поддержки отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

В четвертых, путем:

- повышения безопасности информационных систем, включая сети связи, прежде всего безопасности первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
- интенсификации развития отечественного производства аппаратных и программных средств защиты информации и методов контроля их эффективности;
- обеспечения защиты сведений, составляющих государственную тайну;
- расширения международного сотрудничества Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

Как видим, обеспечение информационной безопасности – сложная общественно-социальная, правовая, экономическая, научная проблема, решаемая в условиях жестких финансовых, материально-ресурсных, временных и иных ограничений, характерных для сложившейся в России социально-экономической обстановки. Лишь комплексное решение вышеназванных задач и целей одновременно в нескольких плоскостях сможет оказать свое регулирующее воздействие на обеспечение информационной безопасности страны. Работы, проводимые в этой области, должны иметь не только практическую направленность, но и научное обоснование.

В этой связи при исследовании правовой сущности информационной безопасности очень важно понимать, что она представляет собой социальное, а не чисто техническое явление. В связи с этим следует признать не вполне верными взгляды ряда ученых на информационную безопасность как на совокупность, прежде всего, технических мер, направленных на защиту информации, включая так называемые межсетевые экраны, системы контроля доступа, антивирусные программы и другие программные и технические средства и методы. Например, в рамках одной из работ сказано, что «одним из приоритетных направлений политики национальной безопасности является защита информации», в то же время говорится, что «приоритетными объектами правовой защиты в области информационной безопасности выступают права личности и интересы общества в информационной сфере, собственно информация и информационные системы». В данном случае автором отождествляются понятия – защита информации и информационная безопасность, при этом из объектов защиты информационной безопасности исключены интересы государства, что не соответствует предмету национальной безопасности, где информационная безопасность является составной частью [14].

Другие, говоря об информационной безопасности, понимают этот термин узко, как набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных в компьютерных сетях [15].

Третьи под информационной безопасностью подразумевают защищенность информации, обрабатываемой в информационно-вычислительной системе [16].

Безусловно, что информационная безопасность предполагает применение специальных технических средств и методов для защиты информации от несанкционированного доступа, похищения, уничтожения и т.д. Но при этом не должно происходить отождествление указанных понятий. В противном случае неоправданно сужается само понятие информационной безопасности, а соответственно и проблема обеспечения информационной безопасности сводится исключительно к применению технических средств и методов. Следовательно, информационная безопасность это не только защита информации, но и организационные, правовые и другие меры, направленные на обеспечение устойчивого, стабильного развития общества и государства.

При этом более глубокое понимание проблемы различает понятия: информационная безопасность, безопасность информации и защита информации. Как было показано выше, само общее понятие «безопасность», широко употребляемое русским языком, являет собой «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз», и в этой связи ее можно разложить на две составляющие:

- безопасность содержательной части (смысла) информации – отсутствие в ней побуждения человека к негативным действиям, умышленно заложенных механизмов негативного воздействия на человеческую психику или негативного воздействия на иной блок информации (например, информация, содержащаяся в программе для ЭВМ, именуемой компьютерным вирусом);

- защищенность информации от внешних воздействий (попыток неправомерного копирования, распространения, модификации (изменения смысла), либо уничтожения.

Вторая составная часть понятия безопасность информации будет называться защитой информации.

Таким образом, выстраивается ряд из трех научных категорий: информационная безопасность, безопасность информации и защита информации. При этом каждая последующая категория является составной частью предыдущей.

Для более глубокого понимания проблемы мы должны определить еще одно понятие: угроза безопасности.

Категорию «угроза безопасности» личности, общества или государства можно в широком смысле определить как то, что в конечном счете существенным образом может ограничить или нанести ущерб имеющемуся уровню самостоятельности (способности на основе независимо принимаемых решений обеспечивать достижение своих целей, исходя из своих собственных фундаментальных ценностей и функций) данной личности, общества или государства. При таком определении становится очевидным, что сила, и в частности военная сила, традиционно рассматриваемая как основной инструмент политики безопасности, может быть использована лишь в ограниченном и узко определенном числе случаев. А тогда критерием значимости разных форм деятельности в различных общественных сферах является их способность обеспечить достижение обществом своих определенных ценностей и целей.

Безусловно, приведенные рассуждения будут справедливы и в отношении частных видов безопасности, в том числе информационной.

Таким образом, возможны два различных взгляда на проблему обеспечения информационной безопасности: более узкий (традиционный), предусматривающий предотвращение только физического ущерба информационному потенциалу (воздействие на информационные системы и сети) за счет применения любых технических средств, и более широкий, основанный на выше сформулированном понятии угрозы безопасности и не ставящий во главу угла только защиту от технического или другого разрушающего воздействия. В целом именно к этому сводится в своей основе расхождение двух основных подходов к проблеме информационной безопасности ее основных выразителей – России и США.

С учетом рассмотренных признаков категории «безопасность» полагаем необходимым проанализировать, как определяются понятия «информация» и «информационная безопасность» правовыми доктринами этих двух стран. Как нами отмечалось выше, у определений этих двух

понятий в любом их изложении есть (в ряду прочих) одно общее свойство – они до сих пор не являются устоявшимися и общепринятыми. Почему это относится к «информации», мы подробно рассмотрели в первом параграфе – к сожалению, до сих пор не удается до конца точно определить это фундаментальное понятие. Столь же объективны трудности в определении понятия «информационная безопасность»?

Информация:

Россия	США
1. Сообщение, осведомление о положении дел, сведения о чем-либо, передаваемые людьми [17]. 2. Сведения (сообщения, данные) независимо от формы их представления [18].	1. Факты, данные или сообщения в любых условиях или форме. 2. Значение, которое человек придает данным посредством известных соглашений, используемых в их представлении [19].

Информационная безопасность:

Россия	США
1. Состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [20]. 2. Состояние защищенности основных интересов личности, общества и государства в информационном пространстве ¹ , включая информационно-телекоммуникационную инфраструктуру и собственно информацию в отношении таких ее свойств, как целостность, объективность, доступность и конфиденциальность [21]. 3. Состояние защищенности национальных интересов страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз [22].	Обеспечение защиты информации и информационных систем от неавторизованного доступа или изменения информации при ее хранении, обработке или передаче и противодействие отказу от обслуживания авторизованных пользователей или обеспечению обслуживания неавторизованных пользователей. Информационная безопасность включает необходимые меры определения, документирования и предотвращения таких угроз. Информационная безопасность состоит из компьютерной безопасности и безопасности сетей связи [23].

Чтобы разобраться, обратим внимание на принципиальное отличие этих понятий: если российская сторона определяет сам предмет, то американская сторона характеризует его конкретное состояние, причем в определенных внешних обстоятельствах условиях, а именно условиях наличия потенциального или актуального воздействия на предмет извне. В соответствии с этими подходами определяется и позиция двух стран в вопросах информационной безопасности.

Позиция России² заключается в следующем: «... создается реальная угроза использования достижений в информационной сфере в целях, не совместимых с задачами поддержания мировой

¹ Информационное пространство – сфера деятельности, связанная с созданием, преобразованием и использованием информации, включая индивидуальное и общественное сознание, информационно-телекоммуникационную инфраструктуру и собственно информацию.

² Подтверждается Концепцией национальной безопасности Российской Федерации, отмечающей, что «серьезную опасность представляют собой стремление ряда стран к доминированию в мировом информационном пространстве...», разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним». В соответствии

стабильности и безопасности, соблюдения принципов суверенного равенства государств, мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважение прав и свобод человека...» [24].

А вот как эта позиция характеризуется США [25]. «Соединенные Штаты также полагают, что любое незаконное вмешательство или попытка нарушить или изменить любой аспект их национальных информационных систем представляют собой потенциальную опасность для основных объектов их национальной инфраструктуры, а, значит, и угрозу их национальным интересам... Соединенные Штаты полагают, что всем государствам следует принять на национальном уровне меры, необходимые как для охраны их национальных систем, так и для обеспечения того, чтобы преступники или международные террористы, ... которые пытаются нарушить функционирование этих систем, карались бы за это по всей строгости закона»³.

Здесь, как и при сравнении определений понятий «информация», обращает на себя внимание, что американская позиция рассматривает в качестве объектов информационной угрозы только информационные системы. Вернемся к определению «информации». Если российское определение относит к данному понятию фактически все, что дает представление об объекте, американское ограниченное определение принимает во внимание только факты и семантические значения передаваемых или получаемых данных. В соответствии с этим и информационная безопасность в американской трактовке сводится к защите компьютерных комплексов и сетей связи, то есть представляет собой защиту и оборону информации и информационных систем против несанкционированного доступа или модификации информации, находящейся в процессе хранения, обработки или передачи, а также против прекращения функционирования системы для несанкционированных пользователей.

Таким образом, американская трактовка, по сути дела, сужает российскую. В этом смысле американская и российские позиции не противоречивы, но следует отметить, что российская исчерпывающим образом дополняет и расширяет американскую.

На основании вышеизложенного, можно предложить следующее определение понятия «информационная безопасность». *Информационная безопасность – состояние защищенности личности, общества, государства от информации, носящей вредный или противоправный характер, от информации, оказывающей негативное влияние на сознание личности, препятствующей устойчивому развитию личности, общества и государства. Информационная безопасность это также обеспечивающее устойчивое развитие состояние защищенности информационной инфраструктуры, включая компьютеры и информационно-телекоммуникационную инфраструктуру, и информации, в них находящейся.*

Представляется, что осознать содержательную часть понятия «информационная безопасность» проще всего через задачи и цели ее обеспечения.

Наиболее значимые задачи обеспечения национальной безопасности России в информационной сфере изложены в Концепции национальной безопасности Российской Федерации. Ими являются:

- установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;
- совершенствование информационной инфраструктуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную инфраструктуру;
- разработка соответствующей нормативной базы и координация деятельности федеральных органов государственной власти, решающих задачи обеспечения информационной безопасности;

с этим в ряду важнейших задач обеспечения информационной безопасности Российской Федерации значится «противодействие угрозе развязывания противоборства в информационной сфере».

³ Примечательно, что это было написано спустя менее года после утверждения и придания гласности документа, носящего название «Объединенная доктрина информационных операций», в котором в практическом плане рассматриваются вопросы интеграции и синхронизации наступательных и оборонительных информационных операций ... в поддержку военных действия на стратегическом, оперативном и тактическом уровнях».

- развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;
- защита государственного информационного ресурса и, прежде всего, в федеральных органах государственной власти и на предприятиях оборонного комплекса.

Указанные задачи в определенной мере солидаризируются с целями обеспечения информационной безопасности Российской Федерации, сформулированными (авторами проекта Концепции нормативного правового обеспечения информационной безопасности Российской Федерации) Г.В. Емельяновым и А.А. Стрельцовым [26]. Данные авторы выделяют три группы целей:

- а) в гуманитарной области:
 - соблюдение конституционных прав и свобод граждан в области получения информации и обмена ею;
 - защита национальных духовных ценностей;
 - пропаганда национального культурного наследия, норм морали и общественной нравственности;
 - обеспечение права граждан на получение достоверной информации;
- б) в области развития информационной инфраструктуры:
 - развитие отечественной индустрии средств информатизации, телекоммуникации и связи, обеспечение выхода ее продукции на мировые рынки;
 - эффективное использование отечественных информационных ресурсов;
- в) в области обеспечения безопасности информационной инфраструктуры и ресурсов:
 - обеспечение безопасности информационных ресурсов;
 - обеспечение безопасности информационных и телекоммуникационных систем, как развернутых, так и создаваемых на территории России.

Представляется, что юридическая наука в той или иной мере должна принимать участие в решении всех вышеперечисленных задач и реализации соответствующих целей обеспечения информационной безопасности. Однако полагаем, что ее приоритет, решающая роль просматривается в двух областях:

- во-первых, в определении разумного баланса между правом субъектов на свободное получение информации путем ее сбора или доступа к имеющимся ресурсам и правом субъектов на установление ограничений в указанных действиях со стороны иных лиц по отношению к сведениям, обладателями которых они являются;
- во-вторых, разработке и реализации правовых мер защиты информации, доступ к которой должен ограничиваться по правомерным основаниям, а также в обеспечении сохранности информационных ресурсов.

Подводя итог сказанному, можно заключить:

Задачи построения гражданского общества в Российской Федерации как общества информационного, возрастание роли информации, информационных ресурсов и технологий в XXI веке выводят вопросы информационной безопасности России на первый план в системе обеспечения национальной безопасности страны. Именно информация выступает основным связующим звеном всех компонентов государственной политики в единое целое. Укрепление информационной безопасности названо в Концепции национальной безопасности Российской Федерации в числе важнейших долгосрочных задач.

Информационная безопасность представляет собой социальное, а не чисто техническое явление. Ее нельзя отождествлять с применением специальных технических средств и методов для защиты информации от несанкционированного доступа, похищения, уничтожения и т.д. Обеспечение информационной безопасности - это не только защита информации, но и организационные, правовые и другие меры, направленные на обеспечение устойчивого, стабильного развития общества и государства, при которых достигаются следующие цели: конфиденциальность критической информации; целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода); доступность информации, когда она нужна; учет всех процессов, связанных с информацией.

Менее широким и емким по содержанию, нежели информационная безопасность, является понятие «безопасность информации». Эту категорию можно «разложить» на две составляющие: безопасность содержательной части (смысла) информации и защищенность

информации от внешних воздействий (попыток неправомерного копирования, распространения, модификации (изменения смысла) либо уничтожения).

Вторая составная часть понятия безопасности информации представляет собой защиту информации.

Таким образом, содержательная часть категории «информационная безопасность» выстраивается в линию из трех научных категорий: информационная безопасность, безопасность информации и защита информации. При этом каждая последующая категория является составной частью предыдущей.

Информационная безопасность - сложное и до конца не устоявшееся явление, которым обуславливается различие подходов к формулированию этого понятия. Сравнительный анализ российской и американской позиций к определению сущности информационной безопасности позволил понимать под информационной безопасностью состояние защищенности личности, общества, государства от информации, носящей вредный или противоправный характер, от информации, оказывающей негативное влияние на сознание человека, препятствующей устойчивому развитию личности, общества и государства. Информационная безопасность это также обеспечивающее устойчивое развитие состояние защищенности информационной инфраструктуры, включая компьютеры и информационно-телекоммуникационную инфраструктуру, и информации, в них находящейся.

Осознать содержательную часть понятия «информационная безопасность» проще всего через задачи и цели ее обеспечения. Стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности формируются на основе национальных интересов Российской Федерации в информационной сфере и солидаризируются с целями обеспечения информационной безопасности России в трех сферах: гуманитарной, в области развития информационной инфраструктуры, в области обеспечения безопасности информационной инфраструктуры и ресурсов. Наиболее значимые из них изложены в Концепции национальной безопасности Российской Федерации и Доктрине информационной безопасности Российской Федерации.

Юридическая наука должна принимать участие в решении всех поставленных задач и реализации соответствующих целей обеспечения информационной безопасности. При этом ее приоритет должен обеспечиваться в двух областях:

- во-первых, в определении разумного баланса между правом субъектов на свободное получение информации путем ее сбора или доступа к имеющимся ресурсам и правом субъектов на установление ограничений в указанных действиях со стороны иных лиц по отношению к сведениям, обладателями которых они являются;

- во-вторых, разработке и реализации правовых мер защиты информации, доступ к которой должен ограничиваться по правомерным основаниям, а также в обеспечении сохранности информационных ресурсов.

Литература:

1. Лопатин В.Н. Проект концепции военной реформы // Правительственный вестник. - 1990. - № 48.
2. Федоров А.В. Международная информационная безопасность: проблема общего подхода. / Материалы круглого стола: «Глобальное информационное общество и проблемы информационной безопасности»/ Институт Европы РАН. М., 2003.
3. Большая советская энциклопедия. Изд. 2-е. Т. 4. - С. 388.
4. Даль В. Толковый словарь живого великорусского языка. Т.1. - М.: Русский язык. - 1989. - С. 67.
5. Ожегов С.И. Словарь русского языка. - М.: Русский язык. - 1990. - С. 47.
6. Белая книга российских спецслужб. - М.: Обозреватель. 1996. - С. 113;
7. Серебрянников В., Хлопьев А. Социальная безопасность России. - М. ИСПИ РАН. - 1996. - С. 16.
8. Кураков Л.П., Смирнов С.Н. Информация как объект правовой защиты. - М.: Гелиос. - 1998. - С. 18.
9. Концепция национальной безопасности Российской Федерации. Утверждена Указом Президента РФ от 17.12.97, № 1300 // Российская газета от 26.12.97.

10. Лопатин В.Н. Информационная безопасность в системе государственного управления (теоретические и организационно-правовые проблемы). Автореф. дисс. канд. юрид. наук. СПб. - 1997;
11. Бачило И.Л., Лопатин В.Н. Информационное право /Под ред. Топорнина Б.Н.; СПб.: Юридический центр-пресс; 2001. - 789 стр. - С.408.
12. Лопатин В.Н. Информационное общество и правовое государство // Сборник материалов международной конференции «Безопасность информации». - М. - 1997. - С.3.
13. Доктрина информационной безопасности (утв. Президентом РФ (сентября 2000 г. № Пр-1895) [Электронный ресурс] Режим доступа: <http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=28679>.
14. Ярочкин В.И. Информационная безопасность: Учеб. пособие. - М.: Междунар. отношения: Летописец, 2000. - 399 с.
15. Введение в информационную безопасность. Компьютеры: преступления, признаки уязвимости и меры защиты. М., 1998. - [Электронный документ]. - Режим доступа: <http://www.224text.info/index.php??open=T35I7&size=1>.
16. Информационная безопасность государственных организаций и коммерческих фирм. Справочное пособие. Под общей редакцией Л. Д. Реймана. - М.: НТЦ ФИОРД-ИНФО, 2002. - С.13.
17. Философский энциклопедический словарь/ Гл. редакция: Л. Ф. Ильичёв, П. Н. Федосеев, С. М. Ковалёв, В. Г. Панов — М.: Сов. Энциклопедия, 1983.
18. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»//Российская газета. -2006. - 29 июля.
19. U.S. DOD. Dictionary of Military Terms.
20. Доктрина информационной безопасности РФ.
21. Доклад Генерального секретаря ООН 54 сессии ГА ООН «Достижения в сфере информатизации и телекоммуникаций в свете международной безопасности», материалы российской стороны.
22. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. СПб.:, 2000. С.79
23. U.S. DOD. Dictionary of Military Terms. [электронный ресурс]. - Режим доступа: <http://www.pircenter.org/data/publications/yk5-2002.pdf>
24. Пятьдесят четвертая сессия Генеральной Ассамблеи ООН. Доклад Генерального секретаря «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». - Нью-Йорк. - 1999. - С.15.
25. Там же. С.23.
26. Емельянов Г.В., Стрельцов А.А. Информационная безопасность России: Учебное пособие / Под ред. Прохожева А.А. – М.: Всероссийский научно-технический информационный центр, 2000.