# ПРАВОВЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**О.С. Скрементова, кандидат юридических наук, доцент.**
**Санкт-Петербургский университет ГПС МЧС России**

Изучены правовые вопросы обеспечения информационной безопасности в Российской Федерации. Исследованы такие правовые категории, как информационная безопасность, виды информационной безопасности, задачи и методы обеспечения информационной безопасности. Рассмотрены государственная политика информационной безопасности и организационная основа системы ее обеспечения.

*Ключевые слова:* информация, информационная безопасность, внутренняя политика, защита информации, государственная политика, правовое обеспечение

LEGAL ISSUES OF IT SECURITY ENSURING

O.S. Skrementova.
Saint-Petersburg university of the State fire service EMERCOM of Russia

Legal issues of IT security ensuring in the Russian Federation are studied. Such legal categories, as IT security, types of IT security, a tasks and methods of IT security ensuring are investigated. Also state policy of IT security and organizational base of the system of its ensuring are considered.

*Key words:* information, IT security, internal policy, information protection, state policy

Понятие информационной безопасности в российской юридической терминологии не является устоявшимся по причине отсутствия единого методологического основания, на базе которого только и могут быть определены его сущность, степень необходимости использования и границы применения. Это методологическое основание до сих пор не выработано, что проявляется не только в обсуждении понятия информационной безопасности на страницах учебных и научных изданий, но и в текстах официальных документов, в том числе нормативных актов [1].

Понятие информационной безопасности получило развитие в Доктрине информационной безопасности Российской Федерации, являющейся совокупностью официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности государства. В соответствии с п. 1 Доктрины информационной безопасности под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [2].

В основу доктринального определения информационной безопасности положено родовое понятие безопасности как «состояния защищенности», закрепленное в Законе РФ «О безопасности» [3]. Доктринальная формула объекта защиты соответствует родовому объекту, идентифицированному в Законе РФ «О безопасности» как «жизненно важные интересы».

В Доктрине предпринята попытка структурирования национальных интересов Российской Федерации в информационной сфере на основе их четырех составляющих.

Первая составляющая национальных интересов включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации

и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей в обществе, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов содержит в себе информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике России, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов объединяет в себе 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.

Четвертую составляющую национальных интересов образуют защита информационных ресурсов от несанкционированного доступа и обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Предполагается, что все четыре составляющие национальных интересов в информационной сфере могут рассматриваться как совокупность сбалансированных интересов личности, общества и государства. При этом интересы личности заключаются 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 заключаются в обеспечении интересов личности в информационной сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России. Интересы государства заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются задачи по обеспечению информационной безопасности. Характер данных задач определяется текущим состоянием сферы информационной безопасности с учетом наличия тех либо иных внешних и внутренних угроз конституционным правам и свободам человека и гражданина, интересам общества и государства.

В Доктрине информационной безопасности РФ определены основные задачи по обеспечению информационной безопасности:

– разработка основных направлений государственной политики в области обеспечения информационной безопасности России, а также мероприятий и механизмов, связанных с реализацией этой программы;

– развитие и совершенствование системы обеспечения информационной безопасности, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности России, а также системы противодействия этим угрозам;

– разработка федеральных целевых программ обеспечения информационной безопасности России;

– разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности, а также сертификации этих систем и средств;

– совершенствование нормативно-правовой базы обеспечения информационной безопасности России, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации;

– установление ответственности должностных лиц федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности;

– координация деятельности федеральных органов государственной власти, органов государственной власти субъектов РФ, организаций независимо от формы собственности в области обеспечения информационной безопасности России;

– развитие научно-практических основ обеспечения информационной безопасности России с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности угроз применения «информационного оружия». Под «информационным оружием» понимаются, как правило, средства уничтожения, искажения или хищения информации после преодоления систем ее защиты, ограничения доступа к ней надлежащих пользователей, дезорганизации работы технических средств.

– разработка и создание механизмов формирования и реализации государственной информационной политики России;

– разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;

– обеспечение технологической независимости России в важнейших областях информации, телекоммуникации и связи, определяющих ее безопасность, и, в первую очередь, в области создания специализированной вычислительной техники для образцов вооружений и военной техники;

– разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и, прежде всего, используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;

– развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;

– создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;

– расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;

– обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;

– создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

Методы обеспечения информационной безопасности делятся на общие и частные. Общие методы, в свою очередь, дифференцируются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности согласно Доктрине относятся разработка нормативных правовых актов, регламентирующих отношения в информационной сфере и нормативных методических документов по вопросам

обеспечения информационной безопасности России. Основными направлениями этой деятельности, в частности, являются:

– законодательное разграничение полномочий в области обеспечения информационной безопасности между федеральными органами государственной власти и органами государственной власти субъектов РФ, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;

– разработка и принятие нормативных правовых актов РФ, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;

– законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;

– определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории России, и правовое регулирование деятельности этих организаций;

– создание правовой базы для формирования в России региональных структур обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности, в частности, являются:

– создание и совершенствование системы обеспечения информационной безопасности России;

– усиление правоприменительной деятельности органов исполнительной власти;

– разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств;

– создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

– выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи;

– сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

– контроль за действиями персонала в защищенных информационных системах.

Экономические методы обеспечения информационной безопасности включают в себя:

– разработку программ обеспечения информационной безопасности России и определение порядка их финансирования;

– совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Частные методы обеспечения информационной безопасности России разделяются на методы, использование которых обусловлено спецификой различных сфер жизнедеятельности общества и государства. В каждой из этих сфер имеются свои особенности, связанные со своеобразием объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности. Доктрина не указывает

прямо на конкретные частные методы, а оперирует объектами, наиболее подверженными воздействию угроз информационной безопасности, и мерами, которые следовало бы принять в сферах экономики, внутренней и внешней политики, науки и техники, духовной жизни, обороны, в общегосударственных информационных и телекоммуникационных системах, в правоохранительной и судебной сферах в условиях чрезвычайных ситуаций.

Государственная политика обеспечения информационной безопасности России базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере. Она определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ в области обеспечения информационной безопасности, порядок закрепления их обязанностей по защите интересов РФ в информационной сфере в пределах установленной компетенции.

В основу государственной политики обеспечения информационной безопасности положены следующие принципы:

– соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности;

– открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов РФ и общественных объединений, предусматривающая информирование общества об их деятельности, с учетом установленных законодательством РФ ограничений;

– правовое равенство всех участников процесса информационного взаимодействия;

– приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов России [4].

Приоритетным направлением государственной политики в области обеспечения информационной безопасности является совершенствование правовых механизмов регулирования общественных отношений, складывающихся в информационной сфере.

В рамках данного направления актуальными предполагаются:

– оценка эффективности применения действующих нормативных правовых актов;

– создание организационно-правовых механизмов обеспечения информационной безопасности;

– определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем;

– создание системы сбора и анализа данных об источниках угроз информационной безопасности;

– разработка нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;

– разработка составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодекс, в законодательство РФ о государственной службе;

– совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности.

В соответствии с Доктриной информационной безопасности РФ первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности РФ являются:

– разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовке концепции правового обеспечения информационной безопасности;

– разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации;

– принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов РФ, обеспечение технологической независимости страны в области создания и эксплуатации информационно-телекоммуникационных систем оборонного значения;

– гармонизация отечественных стандартов в области информатизации и обеспечение информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения.

Система обеспечения информационной безопасности РФ является частью системы обеспечения национальной безопасности страны, призванной к реализации государственной политики в информационной сфере. Реализуя эту политику, система обеспечения информационной безопасности выполняет ряд функций, важнейшими из которых являются:

– разработка нормативной правовой базы в сфере обеспечения информационной безопасности;

– создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;

– оценка состояния информационной безопасности РФ, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;

– координация деятельности государственных органов, решающих задачи обеспечения информационной безопасности РФ;

– предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере;

– развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств;

– проведение единой технической политики в области обеспечения информационной безопасности;

– организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности РФ;

– защита государственных информационных ресурсов;

– осуществление международного сотрудничества в сфере обеспечения информационной безопасности.

Построение системы обеспечения информационной безопасности основано на разграничении полномочий органов законодательной, исполнительной и судебной власти, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов РФ.

Основными элементами организационной основы системы обеспечения информационной безопасности выступают Президент РФ; Совет Федерации; Государственная Дума; Правительство РФ; Совет Безопасности РФ; федеральные органы исполнительной власти; межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ; органы исполнительной власти субъектов РФ; органы местного самоуправления; органы судебной власти; общественные объединения; граждане [5].

Президент РФ в пределах своих полномочий руководит органами и силами по обеспечению информационной безопасности страны; санкционирует действия по обеспечению информационной безопасности; формирует, реорганизует и упраздняет

подчиненные ему органы и силы по обеспечению информационной безопасности; определяет приоритетные направления государственной политики в области обеспечения информационной безопасности и меры по реализации Доктрины.

Палаты Федерального Собрания РФ по представлению Президента РФ и Правительства РФ формируют законодательную базу в сфере обеспечения информационной безопасности.

Правительство РФ координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ и предусматривает выделение средств, необходимых для реализации федеральных программ в области обеспечения информационной безопасности.

Совет Безопасности РФ проводит работу по выявлению и оценке угроз информационной безопасности РФ, готовит проекты решений Президента РФ по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности, координирует деятельность органов и сил по обеспечению информационной безопасности, контролирует реализацию решений Президента РФ.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства РФ, решений Президента РФ и Правительства РФ в области обеспечения информационной безопасности; разрабатывают нормативные правовые акты в этой области и представляют их Президенту РФ и Правительству РФ.

Межведомственные и государственные комиссии решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности РФ.

Органы исполнительной власти субъектов РФ взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства РФ, решений Президента РФ, Правительства РФ в области обеспечения информационной безопасности, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности РФ [6].

Органы местного самоуправления обеспечивают соблюдение законодательства РФ в сфере обеспечения информационной безопасности РФ.

Органы судебной власти осуществляют правосудие по делам о преступлениях, связанных с посягательствами на охраняемые законом интересы личности, общества и государства в информационной сфере и обеспечивают судебную защиту прав граждан и общественных объединений в случае их нарушения.

В состав системы обеспечения информационной безопасности РФ могут входить элементы, ориентированные на решение локальных задач в этой области. Компетенция федеральных органов государственной власти, органов государственной власти субъектов РФ, других государственных органов, входящих в состав системы обеспечения информационной безопасности РФ и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента РФ и Правительства РФ.

**Литература**

1. Бачило И.Л. Методология решения правовых проблем в области информационной безопасности // Информатика и вычислительная техника. 1992. № 2–3.

2. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: учеб. / под ред. Б.Н. Топорнина. СПб., 2005. С. 580–652.

3. Волокитин А.В., Копылов В.А. Информационная безопасность и информационное законодательство // Сборник научно-технической информации. Сер. 1. 1996. № 7.

4. Копылов В.А. Информационное право: учеб. М., 2012. С. 218–231.

5. Фатьянов А.А. Концептуальные основы обеспечения безопасности на современном этапе // Безопасность информационных технологий. 1999. № 1. С. 26–40.
6. Ярочкин В.И. Информационная безопасность: учеб. пособ. М., 2010.