ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ, ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ИНФОРМАЦИОННЫХ РЕСУРСОВ РОССИИ: СОСТОЯНИЕ. НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ.

Загинайлов Ю.Н.
Алтайский государственный технический университет
г.Барнаул, тел. 36-47-38, E-mail: zun@agtu.secna.ru

Система правового обеспечения противодействия угрозам безопасности информационных и телекоммуникационных систем (ИС и ТКС) и информационных ресурсов (ИР) России образуется совокупностью федерального законодательства, законодательства субъектов РФ и международных договоров России.

Основными источниками права в данной области являются:
- федеральные законы, регулирующие отношения в области обеспечения безопасности;
- федеральные законы, регулирующие деятельность отдельных федеральных органов исполнитель ной власти;
- нормативные правовые акты Президента РФ и Правительства РФ по вопросам, связанным с созданием и использованием средств защиты информации и их сертификацией, государственной системой защиты информации в РФ от технических разведок и от её утечки по техническим каналам;
- нормативные правовые акты субъектов РФ, направленные на обеспечение безопасности региональных ИС и ТКС и сетей связи;
- международные (двусторонние и многосторонние) договоры РФ с государствами - участниками СНГ в области защиты информации, обеспечения безопасности закрытой правительственной связи и использования аппаратуры шифрования;
- соглашение с Организацией Североатлантического договора о защите информации.

За последние годы в РФ реализован комплекс мер по совершенствованию правового обеспечения ее информационной безопасности. Начато формирование базы правового обеспечения информационной безопасности. Приняты Закон Российской Федерации "О государственной тайне", Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах, Федеральные законы "Об информации, информатизации и защите информации", "Об участии в международном информационном обмене", ряд других законов, развернута работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Важным шагом в этом вопросе явилось принятие в 2000 году Доктрины информационной безопасности РФ. В этом документе сформулированы угрозы безопасности ИС, ТКС и ИР и направления совершенствования правовых механизмов.

Угрозами безопасности ИС и ТКС, как уже развернутых, так и создаваемых на территории России, могут являться:
- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно - телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно - ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств, для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

На основе анализа современных угроз безопасности ИС и ТКС, ИР и существующего законодательства определены основные недостатки правового обеспечения в этой сфере. К ним относятся:
- диспропорции в развитии федеральной и региональной составляющей национального законодательст ва, наличие противоречий между ними, а также отсутствие законодательной базы для согласования в рассматриваемой области законотворческой деятельности РФ и её субъектов;
- недостаточное правовое регулирование отношений в области развития технологического

обеспечения информационной безопасности РФ;
- неурегулированность вопросов разграничения полномочий между федеральными органами исполнительной власти субъектов РФ в области обеспечения безопасности ИС, ТКС и сетей связи;
- недостаточная эффективность правовых механизмов установления ответственности за правонарушения в сфере обеспечения информационной безопасности ИС, ТКС сетей связи и ИР;
- неразвитость института конфиденциальной информации и защиты этой категории ИР в ИС и ТКС.

Исходя из недостатков разработчиками Доктрины информационной безопасности РФ определены первоочередные мероприятия по совершенствованию правового обеспечения информационной безопасности ИС, ТКС, сетей связи и ИР.

Среди первоочередных мероприятий по совершенствованию правового обеспечения безопасности ИС, ТКС и ИР выделяют две группы:
- совершенствование системы международных договоров и нормативных правовых актов международных организаций, участницей которых является РФ;
- совершенствование федерального и регионального законодательства.

Среди направлений совершенствования системы международных договоров наиболее важными являются:
- предотвращение создания и использования средств нарушения нормального функционирования международных и национальных ИС, ТКС и сетей связи, а также несанкционированного доступа к ИР;
- формирование международной системы обеспечения безопасности глобальных ИС, ТКС и сетей связи, предотвращения использования против них средств нарушения нормального функционирования ИС;
- дальнейшее развитие двусторонних и многосторонних связей с государствами - участниками СНГ и другими государствами, разработка совместных программ в рамках заключённых международных договоров.

Среди направлений совершенствования федерального и регионального законодательства наиболее значимыми являются:
- законодательное разграничение полномочий в области обеспечения информационной безопасности РФ 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 Российской Федерации, 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;
- уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;
- законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;
- определение статуса организаций, предоставляющих услуги глобальных информационно - телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций;
- создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.
- совершенствование системы сертификации современных информационных технологий, средств информатизации, телекоммуникации и связи в соответствии с требованиями безопасности информации;
- совершенствование правового обеспечения оперативно-розыскной деятельности по предупреждению, выявлению и пресечению правонарушений в сфере компьютерной информации;
- регулирование вопросов использования импортных аппаратных и программных средств защиты информации;
- создание условий для развития отечественной индустрии средств защиты информации, обеспечения технологической независимости России в важнейших областях информатизации;
- развитие, с использованием информационно - телекоммуникационных ситем и сетей связи, современной защищённой технологической основы управления государством в мирное время, в чрезвычайных ситуациях и военное время;
- создание законодательной базы для функционирования государственной системы защиты информации в РФ от технических разведок и от утечки её по техническим каналам;
- дальнейшее развитие законодательства о государственной тайне;
- развитие системы страхования информационных рисков;
- развитие законодательства, регулирующего отношения в области электронного документооборота и использования электронной цифровой подписи;
- развитие законодательства о конфиденциальной информации и системы её защиты;
- разработка методических материалов по определению размера материального ущерба, причиняемого интересам личности, общества и государства правонарушениями в информационной сфере;
- совершенствование правовых механизмов борьбы с правонарушениями в области компьютерной информации.

Правовое обеспечение безопасности информационных, телекоммуникационных систем и информационных ресурсов России - важнейшая составляющая правового обеспечения безопасности всей информационной сферы РФ.