Введение

Вступление человечества в XXI век знаменуется бурным развитием информационных технологий во всех сферах государственной деятельности и общественной жизни. Информация все в большей мере становится стратегическим ресурсом любого государства, производительной силой и дорогим товаром. Это не может не вызывать стремления государств, организаций и отдельных граждан получить преимущества за счет овладения информацией, недоступной конкурентам (оппонентам), а также за счет нанесения ущерба информационным ресурсам противника (конкурента) и защиты своих информационных ресурсов.

Понимая значимость обеспечения безопасности государства в информационной области, в сентябре 2000 г. Президентом Российской Федерации была утверждена «Доктрина информационной безопасности Российской Федерации», а в декабре 2015 г. Указам Президента Российской Федерации утверждена «Стратегия национальной безопасности Российской Федерации».

В современных условиях очень остро стоит вопрос информационной безопасности, как на уровне государства, различных организаций, так и на уровне отдельных граждан. В этих условиях важно обеспечить конституционные права граждан на получение достоверной информации, на ее использование в интересах осуществления законной деятельности бизнеса, а также на защиту государственной, коммерческой, семейной, личной, профессиональной и иных видов тайн.

Противоборство государств в области информационных технологий, стремление криминальных структур противоправно использовать информационные ресурсы, необходимость обеспечения прав граждан в информационной сфере, наличие множества случайных угроз вызывают острую необходимость обеспечения защиты информации во всех ее проявлениях.

Проблема обеспечения информационной безопасности на всех уровнях может быть решена успешно только в том случае, если создана и функционирует комплексная система защиты информации, охватывающая как правовые, так организационные аспекты, технические и иные меры, возникающие при защите информации в ходе ее восприятия, обработки, хранения, передачи и создании технических средств и систем, а также средств защиты информации.

Право, правовые нормы являются основой регулирования отношений в области информационной безопасности (защита информации). На нормах права базируются организационные, технические, экономические и морально-этические меры, направленные на исключение или уменьшения угроз (рисков) в информационной области. От знания обязательных требований в области информационной безопасности (защита информации),

установленных в нормативных правовых актах Российской Федерации, во многом зависит их практическая реализация на практике. Опираясь на нормы права юридические лица, индивидуальные предприниматели и физические лица защищают свои интересы от угроз в информационной области.

Важным направлением в обеспечении информационной безопасности (защита информации) принадлежит ее организационное обеспечение. От составления перечня сведений подлежащих защите, порядка допуска и доступа работников к охраняемым сведениям, организации пропускного режима, введения временных, территориальных, частотных и иных ограничений в отношении работников, технических средств и систем и проведение других организационных мероприятий позволит совместно с правовыми и техническими мерами уменьшить угрозы (риски) в информационной области.

Именно эти аспекты и рассматриваются в настоящем учебном пособии. Оно позволит выработать у читателей целостный, системный взгляд на правовые и организационные основы информационной безопасности (защита информации).

Пособие состоит из двух разделов. В первом разделе рассматриваются вопросы правового обеспечения информационной безопасности. Во втором разделе – вопросы организации информационной безопасности.

В гл. 1 рассмотрены роль и место информационной безопасности (защита информации) в системе национальной безопасности государства, сущность и содержание нормативных правовых актов РФ в области информационной безопасности (защита информации), правовая модель информационной безопасности (защита информации), государственная система защиты информации, полномочия, права и обязанности Президента РФ, палат Федерального собрания РФ, Правительство РФ, Совета безопасности России, федеральных органов исполнительной власти и функции органов государственной власти субъектов РФ и органов местного самоуправления в области безопасности, в том числе информационной безопасности (защита информации).

В гл. 2 информация рассматривается как объект правовых отношений в области защиты информации, классификации защищаемой информации по праву собственности и материальным объектам, классификации тайн и их правовой регламентация.

Гл. 3 посвящена государственной системе защиты государственной тайны в Российской Федерации, порядок засекречивания и рассекречивания сведений, составляющих государственную тайну и их носителей и допуска должностных лиц и граждан к государственной тайне, основания для отказа и прекращения допуска.

В гл. 4 содержатся правовые основы защиты коммерческой тайны и конфиденциальной информации, способы охраны конфиденциальной

информации, права и обязанности работника и работодателя по защите конфиденциальной информации.

В гл. 5 освящается сущность и содержание обработки и защиты персональных данных в России, права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные, риски государственных органов, муниципальных органов, юридических и физических лиц при нарушении нормативных правовых актов РФ в области обработки и защиты персональных данных, организация защиты персональных данных в организации, модель угроз безопасности персональных данных, классификация информационных систем персональных данных и положение об обработке и защите персональных данных в организации..

В гл. 6 перечислены цели, задачи, критерии, основные понятия и принципы в области лицензирования, полномочия и права лицензирующих органов, сущность и содержание сертификации и системы сертификации РФ.

В гл. 7 объяснены сущность и содержание государственного контроля (надзора) и муниципального контроля в РФ, в том числе в области защиты информации и персональных данных.

В гл. 8 рассматриваются вопросы сущности и содержания организационных основ защиты информации, а также организационные мероприятия по обеспечению безопасности информации.

В гл. 9 приведен порядок допуска должностных лиц и граждан к коммерческой тайне и иной видам тайн и основания для отказа и прекращения допуска должностных лиц и граждан к коммерческой тайне.

Гл. 10 посвящена организации конфиденциального делопроизводства в организации и сущности и содержания электронного документооборота.

Гл. 11 рассказывает о физической защите объектов и пропускного режима в организации.

В гл. 12 описаны сущности, содержания, виды и способы аудита информационной безопасности (защита информации).

Авторы заранее приносят извинения за возможные неточности в изложении отдельных положений нормативных правовых актов в связи с оперативным внесением в них изменений и дополнений, а также неполные ссылки на труды авторов, работающих в этой области, и на интернет-ресурсы.

Авторский коллектив не претендует на исчерпывающее изложение всех правовых и организационных мер по обеспечению информационной безопасности (защита информации) и с благодарностью воспримет предложения и замечания читателей.