Информационная безопасность и правовые методы ее защиты

Федеральным законом от 27.07.2006 № 149-ФЗ регулируются отношения в сфере информации, информационных технологиях и о защите

Особое регулирование применяется в отношении трех видов информации:

· сведений, отнесенных к государственной тайне;

· конфиденциальной документированной информации;

· персональных данных.

Следует отличать информацию, работающую в режиме тайны, от информации соотносящейся со способностью лица к полезной деятельности, т.е. знаний, навыков, умений, которые не могут быть использованы без него. Например, это деловые качества работника – способности выполнять трудовую функцию с учетом профессионально-квалификационных и личностных качеств. Использование своих профессиональных навыков и умений даже при работе у другого работодателя не является нарушением конфиденциальности.

Нормативно-правовые документы регулирующие защиту информации

Основополагающим законом является Федеральный закон РФ «О информации, информационных технологиях и о защите информации».

Статья 16 Закона характеризует понятие «Защита информации» и определяет её направленность на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- соблюдение конфиденциальности информации ограниченного доступа;

- реализацию права на доступ к информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Закон устанавливает обязанности обладателей информации и операторов информационных систем.

Эти обязанности сводятся к обеспечению:

1. предотвращения несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2. своевременного обнаружения фактов несанкционированного доступа к информации;

3. предупреждению возможности неблагоприятных последствий нарушения порядка доступа к информации;

4. недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование.

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

Статья 183. УК РФ предусматривает наказание за незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

Организационно-правовые формы защиты государственной тайны

Федеральным законом «Об информации, информатизации и защите информации» определено, что государственные информационные ресурсы Российской Федерации являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа.

Понятие государственной тайны определено в Законе «О государственной тайне» как «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации» (ст. 2).

Таким образом, исходя из баланса интересов государства, общества и граждан, область применения Закона ограничена определенными видами деятельности: военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной.

Общая организация и координация работ в стране по защите информации, обрабатываемой техническими средствами, осуществляется коллегиальным органом – Федеральной службой по техническому иэкспортному контролю (ФСТЭК) России при Президенте Российской Федерации, которая осуществляет контроль за обеспечением в органах государственного управления и на предприятиях, ведущих работы по оборонной и другой секретной тематики.

Проблемы, связанные с повышением безопасности информационной сферы, являются сложными, многоплановыми и взаимосвязанными. Они требуют постоянного, неослабевающего внимания со стороны государства и общества. Развитие информационных технологий побуждает к постоянному приложению совместных усилий по совершенствованию методов и средств, позволяющих достоверно оценивать угрозы безопасности информационной сферы и адекватно реагировать на них.