Нормативно-правовое регулирование информационной безопасности

В состав законодательства по обеспечению информационной безопасности включаются федеральные законы, подзаконные нормативные правовые акты федеральных органов исполнительной власти, законы и подзаконные нормативные правовые акты субъектов Российской Федерации.

К числу наиболее значимых нормативных правовые актов в области обеспечения информационной безопасности относятся следующие законы и подзаконные акты.

Конституция Российской Федерации содержит нормы, которые определяют правовые основы информационной безопасности: основные положения правового статуса субъектов информационных отношений, принципы информационной безопасности (законности, уважения прав, баланс интересов личности, общества и государства), конституционный статус государственных органов, обеспечивающих информационную безопасность и др.

Например, к таким положениям относятся нормы, которые устанавливают право каждого субъекта свободно искать, получать, передавать, производить и распространять информацию любым законным способом (п.4.ст. 29).

Это конституционное право, устанавливающее возможность удовлетворения интересов личности и общества сбалансировано необходимостью их ограничения федеральным законом в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (п.3.ст.55).

Конституция Российской Федерации устанавливает запрет на доступ к информации о частной жизни и передачу сообщений по линиям телефонной связи (ст.23).

Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности» (87)закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

Закон определяет ключевые термины в области безопасности, которые применимы и для сферы информационной безопасности, принципы и систему безопасности, правовой статус и состав Совета Безопасности Российской Федерации.

Федеральный закон от 27.07.2006, г., № 149-ФЗ «Об информации, информационных технологиях и о защите информации»(88)фиксирует базовые нормы для всей системы информационного законодательства, в т.ч. правового обеспечения информационной безопасности. Они определяют *основные термины* и их определения, *принципы правового регулирования* отношений в сфере информации, информационных технологий и защиты информации (ст.3), *классификацию информации* по категориям доступа — общедоступную и ограниченного доступа (ст. 5), порядку ее предоставления или распространения (свободно распространяемую, обязательного предоставления или распространения, ограниченного распространения или запрещаемую для распространения вообще). Закон определяет базовые положения правового режима *доступа к информации* (ст.8) *и его ограничения* (ст.9), основные *параметры правовых режимов* распространения (ст.10) и документирования (ст.11) информации, информационных систем (ст.13), информационно-телекоммуникационных сетей (ст.15) и общие *условия защиты* информации (ст.16), информационных систем (ст.13) и использования информационных технологий, а также в общих чертах описывает *ответственность за правонарушения* в сфере информации, информационных технологий и защиты информации.

Федеральный закон от 21 июня 1993 № 5485–1 «О государственной тайне», Федеральные законы от 29 июля 2004 № 98-ФЗ «О коммерческой тайне» и от 27.07.2006 г. № 152-ФЗ «О персональных данных» **(89, 90, 91)** устанавливают правовые

режимы информации ограниченного доступа, в том числе, сведений, составляющих государственную и коммерческую тайну.

Нормы названных законов на более конкретном уровне, чем норма ст.9 закона «Об информации» регулируют формирование условий правового режима доступа к сведениям конфиденциального характера, конкретизируют правовой статус субъектов отношений, возникающих по поводу тайн и персональных данных. Именно в названных законах содержатся основные запреты, ограничения и дозволения, которые составляют правовые основания для формулировок составов информационных правонарушений, направленных на интересы личности, общества и государства в области конфиденциальности информации.

Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (92).Нормы названного закона определяют правовой режим технологического обеспечения защиты информации в системе базовых законов информационного законодательства. В ст. 1 этого закона определена его цель - *обеспечение правовых условий* использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. В законе сформулированы функции электронной цифровой подписи: удостоверяющая, защитная и устанавливающая.

Уголовный кодекс РФ в главе 28 Кодекса предусматривает ответственность за совершение преступлений в сфере компьютерной информации (ст.272-275). Всего в тексте Кодекса содержится более *50 отдельных статей*, устанавливающих уголовную ответственность за нарушение установленных запретов в информационной сфере.

Трудовой кодекс РФ устанавливаетправовой режим персональных данных работника, определяет общие требования по их обработке и защите, устанавливает сроки хранения таких данных и процедуру их использования. В случаях нарушения норм, регулирующих получение, обработку и защиту персональных данных работника, виновные лица привлекаются к дисциплинарной, материальной, административной, гражданско-правовой и уголовной ответственности. Трудовой кодекс РФ определяет норму об ответственности за разглашение отдельных видов тайн и персональных данных.

КоАП РФ в главе 13 определяет административную ответственность за правонарушения в области связи и информации посвящена отдельная глава (ст. 13.1-13.24). В него включены еще более 90 статей, в которых определяется ответственность за совершение проступков информационного характера. Так, например, устанавливается ответственность за отказ в предоставлении гражданину информации (ст. 5.39), за сокрытие или искажение экологической информации (ст. 8.5), за незаконные действия по получению и (или) распространению информации, составляющей кредитную историю (ст. 5.53).

Имеется также массив *нормативных правовых актов подзаконного характера*, состоящий из большого количества документов, регулирующих отдельные направления правового обеспечения информационной безопасности.

Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»(93). В данном Указе устанавливается запрет подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну к информационно-телекоммуникационным сетям международного информационного обмена. В целях защиты информации государственные органы обязаны использовать только средства защиты информации, прошедшие сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данных требований Указа в полной мере должно обеспечить защиту информации, составляющей государственную тайну.

Приказом ФСО России от 07.08.2009 N 487 утверждено ***Положение о сегменте информационно-телекоммуникационной сети Интернет***(94) для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Эксплуатацию, поддержание и развитие сегмента информационно-телекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации обеспечивает Служба специальной связи и информации ФСО России.

В соответствии с названным нормативным правовым актом Сегмент сети Интернет — это находящаяся в ведении (эксплуатации) Федеральной службы охраны Российской Федерации (далее именуется — оператор сегмента сети Интернет) *часть информационно-телекоммуникационной сети, связывающей информационные системы, информационно-телекоммуникационные сети различных государств посредством сетевых адресов информационно-телекоммуникационной сети Интернет* (далее именуется — сеть Интернет).

Сегмент сети Интернет предназначен для обеспечения размещения информации о деятельности Администрации Президента Российской Федерации, Аппарата Совета Федерации Федерального Собрания Российской Федерации, Аппарата Государственной Думы Федерального Собрания Российской Федерации, Аппарата Правительства Российской Федерации, аппаратов Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, Высшего Арбитражного Суда Российской Федерации, Генеральной прокуратуры Российской Федерации и Следственного комитета при прокуратуре Российской Федерации, федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, а также для доступа к сети Интернет должностных лиц указанных государственных органов (далее именуются — пользователи сегмента сети Интернет).

Функционирование сегмента сети Интернет обеспечивается путем применения стандартных протоколов сети Интернет и регламентов обмена информацией в порядке, определяемом оператором сегмента сети Интернет.

В российском правовом пространстве длительное время в обороте используется «служебная информация ограниченного распространения» о деятельности органов государственной власти, которая нередко упоминается в нормативных правовых актах как «служебная тайна». *Постановление Правительства РФ № 1233 от 3 ноября 1994 г. «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах государственной власти» (95)* определяется правовое положение информации ограниченного доступа, несмотря на то, что п.п.1 и 4 ст.9 ФЗ «Об информации» ограничение доступа к информации и, в частности, отнесение информации к сведениям, составляющим служебную тайну, устанавливаются исключительно федеральными законами. Явное несовершенство информационного законодательства и практики его применения отрицательно влияет на состояние правовой защиты интересов субъектов правоотношений. Пробел в нормативных правовых актах, устанавливающих оборот информации служебного характера, не позволяет установить запрет либо ограничения на ее использование, а вместе с этим создает ситуацию невозможности установить административную и / или уголовную ответственность за нарушения порядка распространения этой важной формы информации.