

ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

к.т.н. Ключин Д.И.

Макарова Н.А.

Оренбургский филиал ИЭ УрО РАН

г. Оренбург, Россия

Одним из факторов успешной модернизации экономики Оренбуржья является активное применение современных информационных технологий.

Информация, выступающая объектом информационных отношений, может быть самой различной, от простого электронного сообщения или публичного произведения, до документов содержащих конфиденциальные сведения. Когда мы ведем речь о защите информации, в основном имеем в виду, что она уже обработана, внесена в память компьютера и существует в оцифрованной форме. Информационная система, в которой находится информация, существует на основе технического средства – электронной компьютерной сети, технической связи между компьютерами различных субъектов, между которыми и возникают правоотношения.

Резкое увеличение объёмов информации в региональных информационных системах, рост межведомственного документооборота, развитие информационно-технологической инфраструктуры в субъектах Российской Федерации, объективно требуют эффективной защиты.

Одним из основных способов обеспечения информационной безопасности Российской Федерации является защита информации.

Система нормативных правовых актов Российской Федерации в области защиты информации включает в себя законы, подзаконные акты (указы и распоряжения Президента Российской Федерации и постановления и распоряжения Правительства Российской Федерации, нормативные правовые акты федеральных органов исполнительной власти), а также ряд двусторонних и многосторонних международных договоров Российской Федерации, являющихся согласно Конституции Российской Федерации составной частью ее правовой системы.

Особое место в системе правового регулирования отношений в информационной сфере (в том числе связанных с защитой информации), занимает Федеральный закон «Об информации, информатизации и защите информации» от 27 июля 2006 года № 149-ФЗ (ред. 06.04. 2011) (далее – Закон).

Законом установлены основные правила и способы защиты прав на информацию, защиты самой информации путем принятия основных правовых, организационных и технических (программно-технических) мер по ее защите. Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных.

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой

ограничен федеральными законами (информация ограниченного доступа). Устанавливается перечень информации, доступ к которой не может быть ограничен (например, о деятельности органов власти и об использовании бюджетных средств), информации, предоставляемой на безвозмездной основе.

Закреплен прямой запрет на требование от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и на получение такой информации помимо воли гражданина (физического лица).

В соответствии со Стратегией развития информационного общества в Российской Федерации, утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 (далее – Стратегия), создание информационного общества рассматривается как платформа для решения задач более высокого уровня – модернизации экономики и общественных отношений, обеспечения конституционных прав граждан и высвобождения ресурсов для личностного развития.

Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, утвержденная распоряжением Правительства Российской Федерации от 17 ноября 2008 г. № 1662-р, определяет в качестве целей государственной политики в области развития информационных технологий создание и развитие информационного общества, повышение качества жизни граждан, развитие экономической, социально-политической и культурной сфер жизни общества, совершенствование системы государственного управления, обеспечение конкурентоспособности продукции и услуг в сфере информационных и телекоммуникационных технологий. Для достижения поставленных целей в соответствии с распоряжением Правительства Российской Федерации от 17 ноября 2008 г. № 1663-р утверждены Основные направления деятельности Правительства Российской Федерации на период до 2012 года и перечень проектов по реализации указанных направлений, в том числе проекты в области построения информационного общества, модернизации информационных процессов и качественного развития средств массовых коммуникаций.

Для практической реализации поставленных задач, принята государственная программа «Информационное общество (2011-2020 годы)» утвержденная распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р, (далее – Программа). В соответствии с целями и задачами формирования и развития информационного общества, предусмотренными Стратегией, а также с учетом текущего состояния сферы создания и использования информационных технологий в Российской Федерации целью Программы является получение гражданами и организациями преимуществ от применения информационных технологий за счет обеспечения равного доступа к информационным ресурсам, развития цифрового контента, применения инновационных технологий и радикального

повышения эффективности государственного управления при обеспечении безопасности в информационном обществе. [1]

Одной из задач Программы является создание и развитие специальных информационных и информационно-технологических систем обеспечения деятельности органов государственной власти, в том числе защищенного сегмента сети Интернет и системы межведомственного электронного документооборота.

Без обеспечения безопасности в информационном обществе невозможно реализовать поставленные задачи.

В соответствии со Стратегией развития информационного общества в Российской Федерации, основными направлениями в области противодействия использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам России:

- обеспечение безопасности функционирования информационно-телекоммуникационной инфраструктуры;
- обеспечение безопасности функционирования информационных и телекоммуникационных систем ключевых объектов инфраструктуры Российской Федерации, в том числе критических объектов и объектов повышенной опасности;
- повышение уровня защищенности корпоративных и индивидуальных информационных систем;
- создание единой системы информационно-телекоммуникационного обеспечения нужд государственного управления, обороны страны, национальной безопасности и правопорядка;
- совершенствование правоприменительной практики в области противодействия угрозам использования информационных и телекоммуникационных технологий во враждебных целях;
- обеспечение неприкосновенности частной жизни, личной и семейной тайны, соблюдение требований по обеспечению безопасности информации ограниченного доступа;
- противодействие распространению идеологии терроризма и экстремизма, пропаганде насилия.

В соответствии с Программой обеспечение безопасности в информационном обществе предусматривает:

- противодействие использованию потенциала информационных технологий в целях угрозы национальным интересам Российской Федерации;
- обеспечение технологической независимости Российской Федерации в отрасли информационных технологий;
- развитие технологий защиты информации, обеспечивающих неприкосновенность частной жизни, личной и семейной тайны, а также безопасность информации ограниченного доступа;

– обеспечение развития законодательства Российской Федерации и совершенствование правоприменительной практики в сфере информационных технологий.

В настоящее время в сфере информационных технологий в РФ существует ряд проблем. Отметим некоторые из них.

Высокий уровень зависимости российского рынка от зарубежной продукции в сфере информационных технологий. В подавляющем большинстве создаваемых информационных систем, в том числе и регионах России, сегодня используются в основном зарубежные разработки.

Можно выделить ряд барьеров, препятствующих успешному развитию отечественной промышленности в сфере информационных технологий, среди которых низкий уровень правовой защиты интеллектуальной собственности.

Органы государственной власти субъектов Российской Федерации серьезно отстают от федеральных органов государственной власти по уровню информационно-технологического обеспечения административно-управленческих процессов, а также развития информационно-технологической инфраструктуры и государственных информационных систем.

Наблюдается неконтролируемый рост объемов информации о гражданах, об организациях и объектах хозяйственного оборота, содержащейся в государственных информационных системах, что в условиях отсутствия эффективных механизмов контроля ее использования создает также угрозу нарушения прав граждан.

Необходимо обеспечить инфраструктуру, решения и стандарты в области обмена данными в электронном виде на межведомственном уровне, а также с населением и организациями, что становится особенно актуальным по мере дальнейшего развития государственных информационных систем.

По-прежнему остается низким уровень компьютерной грамотности государственных и муниципальных служащих, что предопределяет актуальность организации непрерывного обучения государственных служащих и оценки навыков использования информационных технологий.

Возрастают угрозы национальной безопасности, среди них:

– увеличение количества компьютерных преступлений, возросла их корыстная направленность, а также наносимый материальный ущерб, увеличилось количество преступлений, в том числе трансграничных компьютерных преступлений, совершенных группами лиц;

– информационные технологии все чаще используются для совершения традиционных преступлений, в частности хищений, вымогательств, мошенничества и террористической деятельности;

– продолжают функционировать и создаваться новые сайты экстремистской и иной противоправной направленности.

В связи с этим, все большую актуальность приобретают вопросы обеспечения безопасности национального сегмента сети Интернет.

В связи с возрастающим числом компьютерных преступлений проблема защиты информации является приоритетной в настоящих условиях. Защита информации должна носить комплексный характер.

Правовое регулирование отношений при обеспечении защиты информации основывается на следующих принципах:

- установление ограничений доступа к информации только федеральными законами;
- обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия. [2]

Статья 5 Закона определяет информацию как объект правовых отношений и в зависимости от категории доступа к ней подразделяет на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа). В зависимости от порядка ее предоставления или распространения подразделяется на информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Обладатель информации, вправе защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами, при осуществлении своих прав обязан: принимать меры по защите информации; ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Статья 9 Закона определяет, что ограничение доступа к информации устанавливается в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой

информации. Она может быть предоставлена третьим лицам в соответствии с федеральными законами или по решению суда.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо его воли.

Отметим, что порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами. Информация, содержащаяся в государственных информационных системах, является официальной. Государственные органы, определенные в соответствии с нормативным правовым актом, регламентирующим функционирование государственной информационной системы, обязаны обеспечить достоверность и актуальность информации, содержащейся в данной информационной системе, доступ к указанной информации в случаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий. [2]

В соответствии с Законом, защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

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

2) соблюдение конфиденциальности информации ограниченного доступа,

3) 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.

Обладатель информации, оператор информационной системы обязаны обеспечить: предотвращение несанкционированного доступа к информации и

(или) передачи ее лицам, не имеющим права на доступ к информации; своевременное обнаружение фактов несанкционированного доступа к информации; предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации; недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование; возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней; постоянный контроль обеспечения уровня защищенности информации.

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, используемых в целях защиты информации, методы и способы ее защиты должны соответствовать указанным требованиям.

Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации устанавливает ст. 17 Закона об информации, в которой указано, нарушение требований влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации.

Привлечение оператора интернет-связи к ответственности за размещенные с его помощью в сети Интернет материалы возможно только в случае наличия его вины (т.е. в случае знания провайдера о существовании нарушения прав правообладателей). Такая практика существует и в европейских странах, согласно ст. 15 Директивы Европейского союза № 2000/31/ЕС «Директива об электронной информации» государства – члены Союза не вправе устанавливать в отношении Интернет-провайдеров каких-либо обязательств по активному повседневному отслеживанию фактов, свидетельствующих о незаконной деятельности в сети Интернет.

По нашему мнению, проблемы связанные с защитой информации, информационных потоков (процессов движения информации) и

информационных систем (как сложных технических объектов, состоящих из технических и программных средств) следует разграничивать, они имеют разную сущность: информационную и техническую. Учитывая, что информация содержится в различных информационных системах, решение проблем информационной безопасности, включая защиту прав обладателя информации и противодействие угрозам национальной безопасности, находится в большой степени в обеспечении безопасного функционирования информационно-телекоммуникационной инфраструктуры, в развитии технологий защиты информации и обеспечении технологической независимости.

Литература:

1. Распоряжение Правительства Российской Федерации от 20 октября 2010 г. № 1815-р г. Москва «О государственной программе Российской Федерации «Информационное общество (2011-2020 годы)»» // Собрание законодательства РФ, 15.11.2010, № 46, ст. 6026.
2. Федеральный закон «Об информации, информатизации и защите информации» от 27 июля 2006 года № 149-ФЗ (ред. 06.04. 2011).