



Паршин К. А., Басыров Р. Р.

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

На сегодняшний день системы электронного документооборота занимают одну из важнейших ролей в делопроизводстве предприятия, позволяя разгрузить бюрократическую машину за счет автоматизации процесса создания, хранения и прохождения всей стадий жизненного цикла документа. Вместе с тем, электронный документооборот порождает новые риски, связанные с конфиденциальностью циркулирующей информации, и пренебрежение защитой обязательно приведет к новым угрозам.

В последние годы спрос на системы электронного документооборота существенно возрос, связано это в первую очередь с законодательством Российской Федерации, регламентирующим переход на системы электронного документооборота для государственных структур, а также положительным опытом их использования в частном коммерческом секторе. Но, внедряя системы электронного документооборота, необходимо уделить существенное внимание безопасности системы. На протяжении многих лет публикуются целые книги о промышленном шпионаже, преступлениях в компьютерной сфере, а наиболее практичные организации уже не один год реализуют написанное на практике.

Ключевые слова: информация, безопасность, система электронного документооборота, защита информации, данные, информационная система, автоматизированная система, персональные данные, конфиденциальная информация.

Parshin K. A., Basyrov R. R.

REGULATORY LANDSCAPE RUSSIAN FEDERATION IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

Today, electronic document management system took a major role in proceedings before the enterprise, will relieve the bureaucracy by automating the process of creating, storing and passing all stages of the life cycle of the document. At the same time, electronic documents gives rise to new risks related to the confidentiality of information circulating and neglect of protection will necessarily lead to new threats.

In recent years, demand for electronic document management system has increased significantly, this is due primarily to the Russian Federation laws regulating the transition to electronic document management systems for government agencies, as well as the positive experience of their use in the private commercial sector. But by implementing an electronic document should be given considerable attention to the security of the system. For many years, published a book about the whole industrial espionage, cyber crime, and the most practical organization for more than a year writing implement in practice

Keywords: information security, electronic document management system, information security, data, information systems, automated system, personal information, confidential information.

При внедрении и использовании систем электронного документооборота на первое место встаёт задача защиты информации, обрабатываемой и хранящейся в системе. Для её решения используется комплекс организационных и программно-технических мер, регламентированных нормативно-правовой базой.

В западных странах уже давно созданы и действуют стандарты, определяющие требования к СЭД: в США – DoD 5015.2-STD (Design Criteria Standard for Electronic Records Management Software Applications); в Евросоюзе – MoReq (Model requirements for the management of electronic records) [3]. Однако в российском законодательстве отсутствуют единые стандарты, требования к системам электронного документооборота, которыми можно было бы руководствоваться при проектировании и/или выборе системы.

Говоря о защищенном электронном документообороте, зачастую подразумевают защиту информации, содержащейся в электронном документе. В этом случае все сводится к защите информации от утечки, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Комплекс мер по организации защиты информации в электрон-

ном документообороте включает в себя: защиту рабочих мест пользователей, защиту сети передачи данных, использование специализированных физических носителей информации и защиту данных на них; а также комплекс организационных мер, определяющих порядок работы с СЭД и циркулирующей в ней информацией ограниченного доступа [4]. На рис. 1 представлены структурные уровни системы электронного документооборота.

К основной базе нормативно-правовых документов, регламентирующих способы и методы защиты информации, можно отнести: Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», данный документ:

- 1) устанавливает основные термины и определения, используемые в информационных технологиях, а также область их применения;
- 2) регламентирует отношения, возникающие в сфере информации, информационных технологий и защиты информации;
- 3) устанавливает правовое регулирование отношений, связанных с использованием информации ограниченного доступа.



Рис. 1. Структурные уровни системы электронного документооборота

Доктрина информационной безопасности Российской Федерации устанавливает виды угроз безопасности информационных и телекоммуникационных средств и систем. Федеральный закон № 63-ФЗ «Об электронной подписи», регулирующий отношения в области использования электронных подписей:

1) определяет понятие ЭП, сертификат ключа проверки электронной подписи, ключ электронной подписи и др.;

2) определяет право использования ЭП и принципы её использования;

3) определяет виды ЭП и области их применения.

Так как в системе электронного документооборота может обрабатываться информация, содержащая персональные данные, следует также отметить Федеральный закон № 152-ФЗ «О персональных данных», регулирующий отношения, связанные:

1) с обработкой персональных данных в системах электронного документооборота;

2) организацией хранения, комплектования, учета и использования содержащих персональные данные документов;

3) предоставлением доступа к сведениям, содержащим персональные данные.

Также необходимо отметить Приказ ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», определяющий состав мер по обеспечению безопасности персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Помимо информации ограниченного доступа, содержащей персональные данные, с СЭД может обрабатываться информация, отнесенная к сведениям, содержащим служебную тайну, в этом случае стоит отметить разработанный проект федерального закона «О служебной тайне», в котором определяются:

1) принцип отнесения сведений к служебной тайне;

2) порядок отнесения сведений к служебной тайне применительно к системам электронного документооборота;

3) порядок снятия ограничений на распространение сведений, составляющих слу-

жебную тайну, применительно к системам электронного документооборота.

Помимо законодательных, существует ряд руководящих документов и ГОСТов, определяющих состав и содержание методик, технических средств и методов реализации защиты информации в СЭД:

- ГОСТ Р 53898-2013 «Системы электронного документооборота. Взаимодействие систем электронного документооборота. Технические требования к электронному сообщению» устанавливает формат, состав и содержание электронного сообщения, обеспечивающего информационное взаимодействие систем управления документами;

- ГОСТ 6.10.4-84 «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники» устанавливает требования к составу и содержанию реквизитов, придающих юридическую силу документам, создаваемым средствами вычислительной техники, а также порядок внесения изменений в эти документы;

- РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», описывающий основные принципы защиты информации от несанкционированного доступа;

- РД «Защита от несанкционированного доступа к информации. Термины и определения» устанавливает термины и определения в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;

- РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации;

- РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов;

- РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации» устанавливает требования к межсетевым экранам.

рованного доступа. Показатели защищенности от несанкционированного доступа к информации» устанавливает классификацию межсетевых экранов по уровню защищенности от несанкционированного доступа к информации;

• РД «Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности» определяет порядок разработки, оценки, регистрации и публикации профилей защиты и заданий по безопасности информационных систем, предназначенных для обработки информации ограниченного доступа.

Также нужно отметить утверждённую заместителем директора ФСТЭК России 14 февраля 2008 г. «Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», предназначенную для использования при проведении работ по обеспечению безопасности персональных данных при их обработке в автоматизированных информационных системах персональных данных.

Делая выводы, можно говорить о том, что нормативная правовая база Российской Феде-

рации в области информационных систем постоянно дополняется и редактируется в соответствии с требованиями информационной безопасности: конкретизируются требования, предъявляемые к ИС в её технической и организационной части, устанавливается порядок лицензирования и сертификации систем, по-полняется классификация возможных угроз и методов их предотвращения. Однако данные нормативно-правовые акты предъявляют требования к информационным системам в целом, и лишь малая их часть относится непосредственно к электронному документообороту, таким образом, в развивающемся информационном обществе встаёт актуальным вопрос создания нормативного акта, регулирующего отношения в области проектирования, разработки и внедрения информационных систем электронного документооборота, учитывающих всю специфику данных систем: хранение и обработка информации ограниченного доступа в совокупности с общедоступной информацией, придание электронным документам юридической силы, условия хранения электронных документов и содержащейся в них информации, взаимодействие разнородных систем при электронном документообмене.

Примечания

1. Стратегия развития информационного общества в Российской Федерации от 7 февраля 2008 г. № Пр-212.
2. Постановление Правительства Российской Федерации от 6 сентября 2012 г. № 890, г. Москва «О мерах по совершенствованию электронного документооборота в органах государственной власти».
3. Жвакина Е. Текущее законодательство в сфере электронного документооборота и СЭД/ЕСМ // ECM-Journal.ru – <http://ecm-journal.ru/docs/Chast-2-Tekushhee-zakonodatelstvo-v-sfere-ehlektronnogodokumentooborota-i-SEhDECM.aspx>
4. Электронный документ и документооборот: правовые аспекты. М.: ИНИОН РАН, 2003.
5. Самодуров А. Особенности защиты электронного документооборота // CNews.ru – <http://www.cnews.ru/reviews/free/security2006/articles/e-docs/>

Паршин Константин Анатольевич, к. т. н, доцент кафедры «Информационные технологии и защита информации», «Уральский государственный университет путей сообщения», Екатеринбург. E-mail: KParshin@usurt.ru

Басыров Руслан Равильевич, Программист 2 категории Управления информатизации, отдел АСУФР, «Уральский государственный университет путей сообщения», 620034, Свердловская обл, Екатеринбург г. Колмогорова ул. 66.

Konstantin Parshin, associate professor of "Information technologies and protection of information" Ural State University of Railway Transport, Ekaterinburg. E-mail: KParshin@usurt.ru

Ruslan Basyrov, Programmer 2 categories of Informatization, Department ASUFR, «Ural State University of Railway Transport», 620034, Sverdlovsk region, Ekaterinburg g, Kolmogorov street, 66. E-mail: rrbasyirov@usurt.ru