

3. Выступление Президента на Первом съезде ученых Беларуси // Официальный Интернет-портал Президента Республики Беларусь [Электронный ресурс]. – 2007. – Режим доступа: <http://www.president.gov.by>. – Дата доступа: 04.11.2007.

4. Ржеутский, Л.Я. Реализация гражданских прав в среде постоянно развивающихся информационных технологий / Л.Я. Ржеутский // Управление в социальных и экономических системах: материалы XIV междунар. научно-практ. конф., Минск, 2006 г. / – МИУ; Е.М. Бобровская (отв. за выпуск) [и др.] – Минск, 2006. – С. 232 – 234.

5. Ржеутский, Л.Я. О построении правового информационного государства / Л.Я. Ржеутский // Проблемы правовой информатизации. – 2007. – № 1. – С. 18 – 22.

НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

О.Ю. Жук

*Белорусский научно-исследовательский центр электронной документации, г. Минск,
Республика Беларусь
OlgaZhuk82@yandex.ru*

Широкое применение информационных технологий в управлении, создание систем электронного документооборота (далее СЭД) как в рамках отдельно взятой организации, так и государства приносит большие преимущества. Однако функционирование СЭД сопряжено с необходимостью обеспечения информационной безопасности систем.

Обеспечение информационной безопасности СЭД имеет три составляющих — технический, организационный и нормативно-правовой аспекты.

Сегодня справедливо обращается внимание на нормативно-правовой аспект защиты информации в СЭД: разработка законодательных механизмов защиты информации и установления юридической ответственности за обеспечение ее сохранности; установление норм и методов защиты авторских прав в информационной сфере; установление единых норм и критериев разработки программного обеспечения и функционирования СЭД; выработка механизмов придания юридической силы электронным документам (далее ЭД) и обеспечения их подлинности и целостности на всех стадиях жизненного цикла; установление правовых норм и юридической ответственности за неправомерное использование средств вычислительной техники [1].

Нормативно-правовую базу в области информационной безопасности в Республике Беларусь составляют «Концепция национальной безопасности Республики Беларусь», законы Республики Беларусь «Об информации, информатизации и защите информации», «О государственных секретах», «Об электронном документе», «Об оценке соответствия требованиям технических нормативных актов в области технического нормирования и стандартизации», «О техническом нормировании и стандартизации» [2]. Отдельные правовые нормы по вопросам защиты информации содержатся в Гражданском и Уголовном кодексах Республики Беларусь, указах Президента, постановлениях Совета Министров, руководящих документах Национального банка, нормативных правовых актах министерств и иных республиканских органов государственного управления.

Так, например, Закон Республики Беларусь «Об информации, информатизации и защите информации» определяет цели, основные требования и меры защиты (правовые организационные, технические), права и обязанности субъектов информационных отношений по защите информации [3].

Закон Республики Беларусь «Об электронном документе» определяет правовые основы применения ЭД, основные требования, предъявляемые к ним, а также права, обязанности и ответственность участников правоотношений в данной сфере [4].

В Законе содержится определение таких понятий как «электронная цифровая подпись» (далее ЭЦП), «средства ЭЦП», «подлинность», «целостность» ЭД. Однако Закон лишь в общих чертах регулирует вопросы, связанные с выработкой и распространением открытых ключей проверки подписи, не определяя статус, функции, обязательства лица, вырабатывающего и распространяющего открытые ключи. Невершенство Закона привело к необходимости пересмотра многих его положений. В проект нового Закона «Об электронном документе и электронной цифровой подписи» включено понятие «удостоверяющий центр», а также перечислены задачи и функции Государственной системы управления открытыми ключами. Удостоверяющий центр определяется как юридическое лицо, осуществляющее издание, распространение и хранение сертификатов открытых ключей и списков отозванных сертификатов открытых ключей. Более подробная регламентация применения ЭЦП, функционирования систем управления открытыми ключами должна идти по пути принятия подзаконных актов технического характера.

Особую часть нормативно-правового обеспечения информационной безопасности составляют технические нормативные правовые акты — стандарты и предстандарты.

Первая группа стандартов — стандарты серии 34.101 (Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий). Стандарты устанавливают общие подходы к формированию требований и оценке безопасности информационных технологий, определяют виды требований безопасности и содержат их систематизированный каталог, критерии и уровни оценки безопасности информационных технологий, позволяющие оценить правильность реализации средств безопасности, стойкость механизмов защиты.

В целом, разработка указанных стандартов осуществляется посредством принятия и использования международных стандартов в качестве национальных. Достоинства подхода — использование лучших мировых практик, повышение доверия при сертификации продуктов и систем, взаимное признание сертификатов. Недостатки — необходимость проведения идентификации текстов, непрерывного отслеживания и внедрения международной нормативной базы, отставание в принятии и использовании стандартов на 3-5 лет, отсутствие собственных методических и инструментальных средств использования отечественной нормативной базы [5].

Вторая группа представлена стандартами по криптографической защите информации — СТБ 1176.1-99 «Информационная технология. Защита информации. Функция хэширования», СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи», применяемыми при разработке средств криптографической защиты и гарантирующими криптостойкость ЭЦП.

Действенное применение стандартов на практике возможно лишь квалифицированными специалистами, что влечет необходимость привлечения сторонних экспертов и увеличение финансовых расходов на защиту. Поэтому развитие технической нормативно-правовой базы связано в большей степени с разработкой методических рекомендаций по обеспечению информационной безопасности СЭД и защиты ЭД на всех стадиях жизненного цикла, а также возможностью их применения специалистами в области делопроизводства и архивного дела, непосредственно работающими с системами электронного документооборота.

Рассмотренная нормативно-правовая база в области обеспечения информационной безопасности является основой построения системы защиты электронного документооборота, в соответствии с которой должны разрабатываться и применяться внутренние локальные нормативные правовые акты организаций, регламентирующие вопросы управления информационной безопасностью СЭД (стандарты организаций, регламенты, инструкции, положения).

Литература

1. Домарев, В.В. Защита информации и безопасность компьютерных систем / В.В. Домарев. — К.: ДиаСофт, 1999. — 480 с.
2. Григорьев, В.Л. Об оценке соответствия автоматизированных систем требованиям безопасности информации / В.Л. Григорьев, Р.В. Млявый // Управление защитой информации №2, Том 11, 2007. — С. 209–218.
3. Об информации, информатизации и защите информации: Закон Респ. Беларусь, 10 ноября 2008 г., № 455-З / Национальный правовой интернет-портал Республики Беларусь [Электронный ресурс]. — 2008. - Режим доступа: <http://pravo.by/webnpa/text.asp?RN=h10800455>.
4. Об электронном документе: Закон Респ. Беларусь, 10 янв. 2000 г., № 357-3 // Национальный реестр правовых актов Республики Беларусь. - 2000. - №7, 2/132.
5. Криштофик, А.М. Состояние и направления развития нормативно-методической базы в области безопасности информационных технологий / А.М. Криштофик, В.В. Анищенко // Управление защитой информации №4, Том 10, 2006. — С.437–448.

АДМИНИСТРАТИВНОЕ РЕГУЛИРОВАНИЕ В РЕСПУБЛИКЕ БЕЛАРУСЬ НАЛОГООБЛОЖЕНИЯ РЕКЛАМЫ НАЦИОНАЛЬНОГО СЕГМЕНТА СЕТИ ИНТЕРНЕТ

Е.Б. Чапко

*Белорусский государственный экономический университет, г. Минск, Беларусь
realgenius@mail.ru*

Интернет-реклама получает все более стремительное развитие и поражает многообразием способов размещения, видов, основными из которых являются баннеры, текстовые блоки, вставки. Реклама в интернете обычно размещается способом наложения, когда совместно с запрашиваемой пользователем