

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

**ДОКУМЕНТОВЕДЕНИЕ И АРХИВОВЕДЕНИЕ:
ТРАДИЦИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ**

Материалы
Всероссийской научно-практической конференции

(Ростов-на-Дону, 8-10 октября 2008 г.)

Ростов-на-Дону 2009

УДК 005.92(075.8)
Д 63

Д 63 **Документоведение и архивоведение: традиции и перспективы развития: материалы Всероссийской научно-практической конференции (Ростов-на-Дону, 8-10 окт. 2008 г.)** – Ростов н/Д: Издательский центр ДГТУ, 2009. – 128 с.

УДК 005.92(075.8)

Печатается по решению редакционно-издательского совета
Донского государственного технического университета

Под редакцией кандидата филологических наук,
доцента кафедры «Документоведение и языковая
коммуникация» ДГТУ
Е.Ю. Кашаевой

© Издательский центр ДГТУ, 2009

специалиста в области электронного документооборота. Понятие «условие» определяется как обстоятельство, от которого что-либо зависит: требование, предъявляемое одной из сторон; соглашение, договоренность; установленные правила; зависимость чего-либо.

Формирование профессиональной компетентности – процесс воздействия, предполагающий некий стандарт, на который ориентируется субъект воздействия; процесс, подразумевающий некую законченность, достижение определенного уровня стандарта; управляемый процесс становления профессионализма, т.е. это образование и самообразование специалиста.

Ж.Н. Колчерина, Я.Г. Вичужанин
Удмуртский государственный университет
г. Ижевск, Россия

Актуальность организационно-правового направления обеспечения информационной безопасности организации в деятельности специалиста по ДОУ

В связи с развивающейся законодательной базой в сфере информационной безопасности все большую актуальность приобретают вопросы обеспечения безопасности информации на предприятиях различных форм собственности и сфер деятельности. Одним из источников информации является документ. Документы – это самая распространенная форма обмена информацией, ее накопления и хранения. Документ отличается разнообразием функционального назначения. Важной особенностью документов является то, что иногда они являются единственным источником важнейшей информации, поэтому их утеря, хищение или уничтожение может нанести непоправимый ущерб.

Ценная информация включается в документы, которые входят в состав информационных ресурсов ограниченного доступа. ФЗ «Об информации, информационных технологиях и защите информации» подразделяет информацию в зависимости от категории доступа на общедоступную и информацию ограниченного доступа, а также в зависимости от порядка ее предоставления или распространения на:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

В свою очередь информацию ограниченного доступа, в соответствии с действующим законодательством, можно классифицировать по виду тайны, а именно на государственную и негосударственную (конфиденциальную информацию), которая представлена разновидностью ее подвидов. Отнесение информации к государственной тайне осуществляется в соответствии с ФЗ «О государственной тайне» № 5485-1. Основные положения данного закона обязательны для исполнения предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами РФ, взявшими на себя обязательства либо обязанные по своему статусу исполнять требования законодательства РФ о государственной тайне. В законе изложены основные организационные, информационные и документационные технологии по работе с информацией и документами, относящимися к государственной тайне, а также основные формы документов, необходимые при соблюдении следующих технологий, а именно:

- порядок отнесения информации к государственной тайне;
- порядок ограничения прав собственности предприятий, учреждений, организаций и граждан РФ на информацию в связи с ее засекречиванием;
- порядок и принципы засекречивания информации и документов;
- описание реквизитов документов, составляющих государственную тайну;
- порядок рассекречивания информации и документов;
- порядок распоряжения информацией и документами;
- порядок передачи информации и документов, составляющим государственную тайну другим государствам;
- организация защиты государственной тайны (органы и их основные функции по защите государственной тайны);
- порядок и организация допуска должностных лиц и граждан к государственной тайне;
- порядок и организация допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием документов и информации, составляющих государственную тайну;
- организация и порядок контроля и надзора за обеспечением защиты государственной тайны.

В действующем законодательстве РФ отсутствует единое понятие конфиденциальной информации, равно как и четкое определение ее

структурного состава. На основе анализа законодательных актов РФ к конфиденциальной информации относятся: коммерческая тайна, служебная тайна, разновидности профессиональной тайны (врачебная тайна, нотариальная тайна, тайна связи и т.п.), банковская тайна и персональные данные и др., каждая из которых имеет свою специфику

В документах как носителях информации информация ограниченного доступа фиксируется, документируется в целях передачи этих сведений во времени и пространстве. Эта информация отображает приоритетные достижения в экономической, политической, военной, научной и других сферах деятельности, разглашение которой может нанести ущерб интересам государства или собственника информации. Разнообразие форм и содержание документов по назначению, направленности, характеру движения и использования является весьма заманчивым источником для злоумышленников, что, естественно, привлекает их внимание к возможности получения интересующей информации.

Деятельность специалистов по документационному обеспечению управления связана с созданием, использованием и хранением значительных объемов информации и документов, образующихся в государственных, муниципальных и частных структурах. Обработываемая информация представляет реальную или потенциальную ценность для учреждения или ее собственника (обладателя) и подлежит защите от различных видов угроз. Защита информации представляет собой деятельность по предупреждению нарушения доступности, целостности, достоверности и конфиденциальности ценных информационных ресурсов, обеспечивающая достаточно надежную безопасность информации в управленческой и производственной деятельности.

Информационная безопасность обеспечивается структурированием информационных ресурсов, ранжированием видов тайн и построением на этой основе целостной системы защиты информации, включающей в себя обязательные элементы: правовой, организационный и инженерно-технический. Инженерно-технический элемент предназначен для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территорий, здания, помещений. Правовой элемент системы защиты информации предполагает правовое регулирование информационных отношений в сфере информационной безопасности организации (предприятия или учреждения). Организационный элемент заключается в регламентации мер управленческого и ограничительного характера, формирующие организацию защиты информации на нормативно-правовой основе. Правила, меры и мероприятия, регламентирующие вопросы доступа, хранения, применения и передачи информации, вводимые в действие административным путем, отражаются в нормативно-методических и

организационно-распорядительных документах организации, учреждения или предприятия. В этой связи целесообразнее использовать единое название двух рассмотренных выше элементов системы защиты информации – организационно-правовой элемент.

Именно эти направления нашли отражение в курсе «Информационная безопасность и защита информации». Курс направлен на формирование у студентов комплексного подхода к осмыслению терминов «информация», «тайна», «безопасность информационная» и «защита информации». Данный подход позволит применить полученные знания в деятельности по выявлению, документированию, использованию и хранению защищаемой информации в организациях, учреждениях и предприятиях различных форм собственности.

Это послужит фундаментом для формирования у студентов основных понятий в области информационной безопасности, а также позволит им применить полученные знания в их непосредственной работе с документами, базами данных, содержащими конфиденциальную информацию.

Н.В. Матвиенко

*Кубанский государственный университет
г. Краснодар, Россия*

Система электронного документооборота как инструмент эффективного управления компанией

Развивающиеся компании сталкиваются с кризисом управления. Управленцы оказываются «засыпаны» все возрастающим потоком задач. Руководство осознает, что нужно что-то изменить, но не знает, что именно нужно менять. Достаточно стандартизировать некоторый набор типовых управленческих решений: проанализировать и выделить в отдельные группы основные процессы организации и прописать их заранее. Огромный объем бумаг вызывает необходимость внедрения системы электронного документооборота.