Плотников М.В., доцент кафедры информатики и ПО НОУ ВПО «Брянский институт управления и бизнеса», e-mail: boinub@online.debryansk.ru

ОРГАНИЗАЦИЯ КОНФИДЕНЦИАЛЬНОГО ДЕЛОПРОИЗВОДСТВА

Организации конфиденциального делопроизводства в информационной безопасности уделяется, как правило, наименьшее внимание, хотя получение конфиденциальной информации через пробелы в делопроизводстве является наиболее простым и малозатратным способом получения информации.

Составные части делопроизводства:

- бумажное делопроизводство;
- электронное делопроизводство;
- системы взаимодействия и сопряжения бумажного и электронного делопроизводства.

При ведении конфиденциального делопроизводства необходимо соблюдать следующие правила [1]:

- присвоение и снятие грифа конфиденциальности должно осуществляться руководством компании;
- обязательная регистрация и учет всех конфиденциальных документов, а также передача их исполнителю под расписку в реестре;
- контроль не только документов, содержащих конфиденциальную информацию, но и бумаг с печатями, штампами, бланками, особенно бланков строгой отчетности, содержащих уникальный номер, зарегистрированных установленным способом и имеющих специальный режим использования;
- организационное выделение конфиденциального делопроизводства из обычного;
- гриф конфиденциальности документа присваивается по наивысшей степени конфиденциальности сведений, в нем изложенных;

- создание конфиденциальных документов производится в изолированных, специально оборудованных помещениях, прием и выдача документов производится через специальное окно, не выходящее в общий коридор или барьер, ограничивающий доступ к рабочим местам лиц, создающих конфиденциальные документы;
- уничтожение конфиденциальных документов, в том числе черновиков, в машинках для уничтожении бумаг (шредерах) в присутствии нескольких человек и с проставлением соответствующих пометок в журналах уничтожения конфиденциальных документов. При большом количестве документов возможно их сжигание;
- запрещение выноса из контролируемой территории конфиденциальных документов;
- к работе с конфиденциальными документами допускаются только лица, заключившие соответствующие договора о нераспространении коммерческой тайны;
- хранение конфиденциальных документов только в сейфах;
- в делах или в архивах конфиденциальные документы должны храниться отдельно от открытых, по завершении оформления дел на последнем листе делается запись о количестве пронумерованных в нем листов, заверенная соответствующей подписью и печатью;
- включать в документы только минимально необходимую конфиденциальную информацию;
- рассылка конфиденциальных документов должна быть обоснованной и сведена к минимуму;
- система учета (ручная или компьютерная) конфиденциальных документов должна предоставлять необходимые удобства поиска и контроля за местонахождением каждого конфиденциального документа;
- организационно исключить необоснованное ознакомление с документами лиц, не имеющих нужных полномочий;
- отправку конфиденциальных документов производить только

заказными или ценными письмами, по каналам специальной связи или осуществлять доставку корреспонденции нарочным из числа сотрудников, допущенных к работе с такими документами;

- контроль за использованием копировально-множительной техники, а также блокирование систем ввода-вывода информации на компьютерах, обрабатывающих конфиденциальную информацию;
- организация периодической проверки делопроизводства.

Порядок создания бумажного делопроизводства

1 этап – создание Секретариата (подразделения, отвечающего за делопроизводство) или введение в штат должности, в чьи функциональные обязанности будет входить обеспечение делопроизводства организации.

2 этап – закупка необходимых принадлежностей для функционирования делопроизводства (сейфы, печати, оборудование помещений и т.д.).

3 этап – создание необходимых нормативных документов (инструкций, должностных обязанностей и т.д.).

4 этап – доведение нормативных документов до сотрудников в рамках функциональных обязанностей.

5 этап - создание механизмов контроля за соблюдением делопроизводства.

6 этап – создание механизма ответственности за нарушение правил делопроизводства.

Делопроизводство должно быть организовано в соответствии с ГОСТами, применяемыми в Российской Федерации. Основа - ГОСТ 6.30–97 «Унифицированные системы документации. Система организационно–распорядительной документации. Требования к оформлению документов» [2,3].

Порядок создания конфиденциального бумажного делопроизводства

1 этап - создание обычного бумажного делопроизводства.

2 этап - определение перечня сведений конфиденциального характера и документов, содержащих конфиденциальные сведения. Разделение сведений на несколько групп по степени конфиденциальности (например: строго

конфиденциальные, конфиденциальные, для служебного пользования).

3 этап - утверждение перечня сведений конфиденциального характера у руководства, а также определение порядка и сроков переутверждения данного перечня, а также снижение и снятие грифа конфиденциальности.

4 этап - определение правил конфиденциального бумажного делопроизводства на основе общего бумажного делопроизводства.

5 этап – определение порядка допуска сотрудников к сведениям конфиденциального характера.

6 этап - заключение договоров о нераспространении конфиденциальных сведений мажду сотрудниками, которые будут допущены к работе с конфиденциальной информацией и руководством организации.

7 этап – создание необходимых нормативных документов (инструкций, должностных обязанностей и т.д.).

8 этап – доведение нормативных документов до сотрудников в рамках функциональных обязанностей.

9 этап - создание механизмов контроля за соблюдением конфиденциального делопроизводства.

10 этап – создание механизма ответственности за нарушение правил конфиденциального делопроизводства.

Составные части бумажного делопроизводства:

Делопроизводство, связанное со стандартными, но специфическими задачами:

- бухгалтерия;
- учредительные документы;
- судебно-процессуальные документы;
- договорные документы и т.д.

Делопроизводство, связанное с текущей деятельностью:

Внешнее делопроизводство:

- доставка входящей корреспонденции (в бумажном виде, в виде факса и т.д.);

- отправление исходящей корреспонденции (в бумажном виде, в виде факса и т.д.);

Внутреннее делопроизводство:

- хранение документов:
- хранение документов у сотрудников;
- хранение документов в Секретариате.
- создание документов у исполнителя;
- издание нормативных документов руководством организации (приказы, распоряжения и т.д.);
- регистрация документа в Секретариате;
- движение документа внутри организации. Создание реестровой системы передачи документов;
- размножение документов (снятие копий);
- контроль за исполнением документов;
- создание архивов документов. Экспертиза ценности документов. Возможность использования в работе документов, определенных в архив;
- уничтожение документов.

Необходимые нормативные документы для функционирования делопроизводства, в том числе конфиденциального:

Нормативно-правовые документы организации с внесенными изменениями и дополнениями, связанными с сохранностью конфиденциальной информации:

- Устав организации;
- “Коллективный договор”;
- правила внутреннего трудового распорядка для сотрудников;
- трудовой договор;
- заключаемые договора.

Договор между руководством организации и сотрудником о сохранении конфиденциальной информации.

Инструкция по обеспечению сохранности конфиденциальной информации в организации. Примерный план инструкции:

- общие положения;
- определение информации и обозначение документов, содержащих конфиденциальную информацию, и сроков ее действия;
- организация работы с конфиденциальными документами;
- порядок сохранности документов, дел и изданий, содержащих конфиденциальную информацию;
- порядок допуска к сведениям, составляющим конфиденциальную информацию;
- контроль за выполнением требований внутри объектного режима при работе со сведениями содержащими конфиденциальную информацию;
- обязанности сотрудников организации, работающих со сведениями представляющими конфиденциальную информацию, и их ответственность за ее разглашение.

Инструкция по организации делопроизводства. Инструкция должна состоять из следующих разделов:

- общие положения;
- правила составления и оформления документов;
- составление и оформление основных видов документов;
- организация документооборота:
- порядок движения и обработки входящих документов;
- порядок движения и обработки исходящих документов;
- порядок движения и обработки внутренних документов;
- регистрация документов;
- контроль исполнения документов;
- систематизация документов;
- разработка номенклатуры дел;
- формирование дел;
- подготовка документов к архивному хранению;

- экспертиза ценности документов;
- описание документов постоянного и временного сроков хранения;
- обеспечение сохранности дел;
- передача дел в архив;
- приложения:
  - примерный перечень документов, не подлежащих регистрации;
  - перечень документов, на которых ставится печать;
  - перечень документов, подлежащих утверждению;
  - перечень документов, подлежащих согласованию;
  - форма регистрационно–контрольной карточки;
  - перечень документов, подлежащих контролю за исполнением, с указанием сроков хранения;
  - акт о выделении к уничтожению документов с истекшими сроками хранения;
  - внутренняя опись документов дела;
  - опись дел, передаваемых на архивное хранение.

Инструкция по конфиденциальному делопроизводству, определяющая:

- порядок выноса-вноса конфиденциальных документов применительно к охраняемой территории;
- порядок работы с конфиденциальными документами вне служебных помещений;
- порядок изготовления и использования бланков организации, печатей и штампов;
- порядок использования бланков строгой отчетности (бланков организации, подготавливаемых за подписью первых лиц организации);
- порядок передачи конфиденциальных документов в случае ухода в отпуск, командировку или увольнение с работы;
- порядок подготовки конфиденциальных документов, его согласование, в том числе с юристами, финансистами, корректорами, а также порядок подписи конфиденциальных документов;

- порядок пересылки конфиденциальных документов вне контролируемых помещений.

Положение о Секретариате (подразделении отвечающего за бумажное и электронное делопроизводство).

Должностные обязанности сотрудников Секретариата по обеспечению делопроизводства.

Корпоративное конфиденциальное электронное делопроизводство должно состоять из следующих взаимосвязанных систем:

- системы электронного конфиденциального документооборота;
- системы защиты информации, циркулирующей в системе электронного конфиденциального документооборота;
- системы электронного конфиденциального информационного хранилища;
- системы сопряжения конфиденциального электронного и бумажного документооборота.

Система электронного конфиденциального документооборота должна предусматривать следующие возможности:

- возможность создания электронных документов с помощью текстовых редакторов, включая создание электронных документов по типовым формам;
- возможность создания составных электронных документов, состоящих из нескольких разных по формату файлов;
- возможность создания электронных документов с помощью сканирования документа на бумажном носителе;
- возможность создания электронных документов с помощью иных электронных данных, полученных с помощью:
- электронной почты;
- корпоративной компьютерной сети;
- устройств ввода компьютерной информации (дисководы и т.д.).
- работу с электронными документами различных форматов (текстовых, графических и т.д.).

- создание регистрационной карточки электронного документа, связки регистрационной карточки с электронным документом и присвоение необходимых реквизитов, среди которых:
  - дата создания, получения, исполнения;
  - регистрационный номер;
  - фамилия, имя, отчество исполнителя, адресата;
  - права доступа;
  - степень конфиденциальности;
  - количество листов и т.д.
- разделения документов по степени конфиденциальности, присвоение каждому документу грифа конфиденциальности и разграничение права пользователей работы с конфиденциальными документами по мандатному принципу.
- получения и отправления электронных документов (документооборот) по корпоративной компьютерной сети, а также по электронной почте.
- работы с взаимосвязанными документами, поддержание возможности установления ссылок между учетными карточками или документами, связанных тематически, отменяющих или дополняющих друг друга (например с помощью гиперссылок с возможностью просмотра цепочки взаимосвязанных документов).
- контроля передвижения электронных документов по сети и контроля ознакомления с электронными документами, а также контроля за копированием, редактированием и размножением электронных документов.
- осуществления контрольных функций (контроля исполнения резолюций, поручений, сроков исполнения и т.д.), а также возможность сигнального режима, как составной части контроля.
- поиска электронных документов по:
  - реквизитам;
  - ключевым словам;
  - содержанию;

- дате создания;
- контрольным срокам;
- исполнителю и т.д.

- анализа электронных документов по:
  - тематике;
  - проблематике;
  - исполнителям;
  - резолюциям;
  - дате создания и т.д.

- дублирования (архивирования) электронных документов с заданной периодичностью, а также ведение систематизированных электронных архивов документов, их образов, учетных карточек с возможностью поиска и анализа.
- разделение конфиденциального и открытого электронного делопроизводства.

Система конфиденциального электронного информационного хранилища должна предусматривать возможность:

- систематизирования поступающих в хранилище документов различных видов и форм и упорядочения работы с ними;
- гарантированно сохранять документы в массивах хранилища, освободив от этой функции сотрудников;
- отслеживать движение документов, выдаваемых сотрудникам, контролировать и обеспечивать их возврат (физические документы) и уничтожение выданных электронных копий;
- обеспечивать эффективный поиск нужных документов в хранилище по идентификационным признакам;
- организовать малозатратную технологию выдачи документов сотрудникам и возврат документов в хранилище;
- уменьшить количество документов, одновременно находящихся у исполнителя за счет оперативного их получения из хранилища;

- упростить работу с документами, находящимися в хранилище, и сократить временные затраты на их подборку и анализ за счет дружественного интерфейса в интерактивном режиме;
- обеспечить режим безопасности документов в процессе их хранения, передачи в хранилище или получения из хранилища за счет использования современных технологий и средств информационной безопасности, а также разграничение доступа пользователей.

Система защиты конфиденциального электронного делопроизводства должна состоять из следующих взаимосвязанных блоков:

- блок технических (программных) средств защиты электронного делопроизводства;
- блок технических средств защиты электронного делопроизводства, связанных с нейтрализацией побочных электромагнитных излучений и наводок;
- блок методов защиты электронного делопроизводства, связанных с человеческим фактором и решением кадровых вопросов;
- блок организационных методов защиты электронного делопроизводства.

Блок технических (программных) средств защиты электронного делопроизводства должен быть многорубежный. Наиболее эффективной является система, состоящая из 3 рубежей:

1 рубеж – системы защиты информации, предусмотренные программным обеспечением, на которой работает компьютерная сеть (средства защиты Windows, Office и т.д.);

2 рубеж – системы защиты информации, встроенные в саму систему электронного делопроизводства;

3 рубеж – системы защиты информации, дополнительно установленные в компьютерной сети на сервере и на рабочих местах пользователя

Блок технических (программных) средств защиты электронного делопроизводства должен предусматривать:

- криптографическую защиту компьютерной информации на магнитных носителях (жестких дисках, дискетах, Zip, CD-ROM и т.д.), в том числе создание защищенных «цифровых сейфов» пользователей на сервере;
- защиту информации (в том числе криптографическими методами) при пересылки по корпоративной компьютерной сети;
- защиту информации (в том числе криптографическими методами) при передаче по электронной почте;
- защиту компьютерной информации от несанкционированного доступа;
- защиту компьютерной сети при работе в глобальной информационной сети Интернет (в идеальном случае для работы с Интернетом, а также с электронной почтой необходим отдельный компьютер, работающий в автономном режиме);
- мандатный принцип доступа пользователей к информационным ресурсам электронного делопроизводства, включающий в себя:
  - контроль и защиту электронного документа от просмотра;
  - контроль и защиту электронного документа от редактирования и отмена защиты от редактирования;
  - контроль и защиту электронного документа от копирования и распечатывания на принтерах;
  - разделение пользователей на группы и наделение каждой группы возможности работы только с электронными документами определенного грифа конфиденциальности
  - контроль целостности и достоверности электронного документа, а также подтверждение авторства исполнителя с помощью электронной цифровой подписи;
  - защиту от вредоносных программ (вирусов);
  - парольную защиту на включение машины, на обращение к жесткому диску и/или на открытие файлов прикладных программ с периодическим изменением используемых паролей.

Системы сопряжения электронного и бумажного делопроизводства

состоят из:

- системы перевода бумажного документа в электронный документ;
- системы перевода электронного документа в бумажный документ;
- системы электронного контроля за бумажным документооборотом;
- системы параллельного хождения одного и того же документа в электронном и бумажном виде.

Представляется целесообразным хождение документа внутри организации осуществлять в электронном виде. Полученные в бумажном виде документы извне сканируются и дальнейшая работа с ними происходит в электронном виде. Полученные извне электронные документы обрабатываются в организации в электронном виде. Перед отправкой исходящие документы (письма, факсы) преобразуются из электронного в бумажное представление и их отправка производятся обычными способами. При необходимости возможна отправка документа и в электронном виде.

ЛИТЕРАТУРА

1.Гавердовский А. Концепция построения систем документооборота. - М.:Ж «Электронный офис». Январь/Февраль 1997.

2.Мельников В.П. и др., Информационная безопасность и защита информации. Учебное пособие для студентов высших учебных заведений.- 3-е изд., стер.– М.: Изд. центр «Академия», 2008. – 336 с.

3.Панкратьев В.В. “Корпоративная безопасность». - Сб. трудов Института бизнеса и делового администрирования Академии народного хозяйства при Правительстве РФ. – М., 2012. с. 350.