Бурдов С. Н.

# Система конфиденциального делопроизводства как форма защиты конфиденциальной информации: нормативные и организационные аспекты

**Бурдов Сергей Николаевич**
Северо-Западный институт управления — филиал РАНХиГС (Санкт-Петербург)
Кафедра конституционного и административного права
Старший преподаватель
208844@list.ru

*РЕФЕРАТ*
В статье рассматриваются нормативные и организационные требования, предъявляемые к построению системы конфиденциального делопроизводства. Выделяются угрозы конфиденциальной информации, которые могут присутствовать в работе российских организаций, а также обосновываются рекомендации для минимизации их возможных последствий.

*КЛЮЧЕВЫЕ СЛОВА*
информация, конфиденциальность, делопроизводство

Burdov S. N.

## The System of Confidential Paperwork as Form of Protection of Confidential Information: Normative and Organizational Aspects

**Burdov Sergey Nikolaevich**
North-West Institute of Management — branch of the Russian Presidential Academy of National Economy and Public Administration (Saint-Petersburg, Russian Federation)
Assistant Professor of the Chair of Constitutional and Administrative Law
208844@list.ru

*ABSTRACT*
The author considers the normative and organizational requirements for building a system of confidential office-work. Highlighted threats to confidential information that may be present in the work of Russian organizations, and also substantiated recommendations to minimize their possible consequences.

*KEYWORDS*
information, privacy, records management

В последнее время проблема защиты информации рассматривается как неотъемлемая составная часть национальной безопасности Российской Федерации. Это ясно определяется стратегией национальной безопасности Российской Федерации[1] и Доктриной информационной безопасности Российской Федерации[2], как и целым рядом других документов.

При этом проблемы, связанные с информационной безопасностью, все чаще затрагивают деятельность различных организаций. При этом причины этого могут

[1] *О Стратегии* национальной безопасности Российской Федерации до 2020 года: Указ Президента РФ от 12 мая 2009 г. № 537 // Собрание законодательства РФ. 18.05.2009. № 20. Ст. 2444.

[2] *Доктрина* информационной безопасности Российской Федерации / Утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895 // Российская газета. 28.09.2000. № 187.

быть совершенно различными. Для государственных организаций, не занимающихся коммерческой деятельностью, необходимость соблюдения режима конфиденциальности информации может касаться тех сведений, распространение которых в соответствии с действующими законодательными актами организации считают нежелательным в интересах обеспечения своей деятельности.

У коммерческих организаций стремление к охране информационных ресурсов и сохранению их конфиденциальности чаще всего обусловлено условиями конкурентной борьбы. Связано это с тем, что на сегодняшний день информация является своеобразным товаром, подчиняющимся законам товарно-денежных отношений [5, с. 17].

Реальный механизм, который может обеспечить защиту документированной конфиденциальной информации, — это создание в организации системы конфиденциального делопроизводства либо, как минимум, применение в открытом делопроизводстве средств и методов, используемых при работе с закрытыми документами. Однако для реализации этого необходимо соблюдение целого ряда принципов.

В первую очередь необходимо отметить, что в отличие от открытого делопроизводства, цель которого состоит в создании справочно-информационной системы, цель учета конфиденциальных документов состоит в сохранности документов и фиксировании их местонахождения.

Вследствие этого система обработки и защиты конфиденциальных документов включает ряд мер, не свойственных открытому делопроизводству. Среди них:

- жесткое регламентирование состава издаваемых документов и контроль процессов документирования начиная со стадии подготовки черновиков и проектов документов;
- создание разрешительной системы доступа к документам и делам, обеспечивающей правомерное и санкционированное ознакомление с ними;
- обязательный поэкземплярный и полистный учет всех без исключения документов, проектов и черновиков;
- учет и обеспечение сохранности не только всех документов, но и учетных форм;
- фиксация прохождения и местонахождения каждого документа, в том числе письменное фиксирование всех обращений персонала к документам;
- контроль копирования и размножения документов;
- регламентация обязанностей сотрудников, в том числе введение персональной ответственности, по работе с документами и защите доверенной конфиденциальной информации;
- проведение систематических проверок наличия конфиденциальных документов, их сохранности и целостности;
- проведение постоянной информационно-аналитической работы, направленной на выявление возникающих потенциальных угроз, определение наиболее оптимальных мер, способствующих укреплению и обновлению системы защиты документированной информации в соответствии с изменяющимися внутренними и внешними обстоятельствами [6, с. 104–106].

Таким образом, конфиденциальное делопроизводство шире открытого и по своим задачам, так как задача открытого делопроизводства состоит в документационном обеспечении управленческой деятельности. Отметим, что целью конфиденциального делопроизводства, кроме того, является и защита документированных сведений, образующихся в процессе конфиденциальной деятельности, а также других объектов, так или иначе связанных с защищаемыми документами.

Конфиденциальные документы должны создаваться только при действительной необходимости в письменном удостоверении их наличия и содержания. При этом решение задач конфиденциальной деятельности должно обеспечиваться минимальным количеством документов при сохранении полноты необходимых сведений.

Конфиденциальной информацией является информация, требующая защиты. Технологии конфиденциального (защищенного) электронного документооборота являются информационными. Информационные технологии, в свою очередь, это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Технологии обработки, хранения, передачи и защиты информации входят в Перечень технологий, имеющих большое социально-экономическое значение, и играют важную роль в обеспечении обороны страны и безопасности государства (критические технологии)[1].

Проблемы защиты информации стали еще более сложными и значимыми в связи с переходом жизненного цикла документированной информации на безбумажную, электронную основу с одновременным применением как «бумажных» технологий делопроизводства и документооборота, так и электронных с использованием автоматизированных информационных систем (АИС).

Защитные мероприятия охватывают не только саму документированную информацию, но и другие объекты, так или иначе связанные с защищаемой информацией (помещения, технические средства обработки и передачи информации и др.).

Технологии конфиденциального делопроизводства и документооборота во многом совпадают с технологиями организации работы с документированной информацией ограниченного доступа, составляющей государственную тайну, которые определены постановлениями Правительства Российской Федерации, например Постановлением Правительства Российской Федерации от 06.02.2010 г. № 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне»[2].

Главное здесь то, что по своей сути они не являются секретными и регулируются общедоступными нормативными правовыми актами о государственной тайне.

Обеспечение сохранности и конфиденциальности документированной информации требует создания и поддержания специальных условий хранения, обработки и обращения документов, гарантирующих надежную защиту как самих документов, так и содержащейся в них информации.

Достигается это путем организации специального режима хранения конфиденциальной информации и обращения с ней, установления разрешительной системы доступа, разработки регламентированной технологии ее создания и обработки [3, с. 305–306].

Руководство конкретной организации (коммерческой, государственной, муниципальной) в пределах своей компетенции определяет:

- категории должностных лиц, уполномоченных относить информацию (документы) к конфиденциальной;
- круг должностных лиц, имеющих доступ к документам и информации различной степени конфиденциальности;
- порядок снятия отметки конфиденциальности с документов, включая электронные, циркулирующие в АИС, иными словами, системах электронного документооборота;
- организацию защиты информации на бумажном носителе;

---

[1] *Об утверждении* перечня технологий, имеющих важное социально-экономическое значение или важное значение для обороны страны и безопасности государства (критических технологий): Распоряжение Правительства РФ от 14.07.2012 г. № 1273-р (ред. от 24.06.2013 г.) // Собрание законодательства РФ. 30.07.2012. № 31. Ст. 4403.

[2] *Об утверждении* Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне: Постановление Правительства Российской Федерации от 06.02.2010 г. № 63 (ред. от 01.11.2012 г.) // Собрание законодательства РФ. 15.02.2010. № 7. Ст. 762.

- организацию защиты информации, циркулирующей в системах электронного документооборота, а также защиту самих автоматизированных информационных систем.

Выполнение задач документационного обеспечения управления также подразумевает под собой обеспечение управленческой структуры полной, своевременной и достоверной документной информацией, организацию исполнения и использование документов. При организации защиты конфиденциальных документов эти задачи расширяются и включают:

- предупреждение несанкционированного доступа любого лица к документу, его частям, вариантам, черновикам, копиям;
- обеспечение физической сохранности документов;
- обеспечение сохранности информации, содержащейся в них.

Выполнение этих задач позволяет не только избежать утраты или подмены документов ограниченного доступа, но и предотвратить нарушение режима их конфиденциальности в результате утечки (разглашения) охраняемых сведений, т. е. несанкционированного (неправомерного) распространения данной информации среди третьих лиц, не входящих в круг субъектов, имеющих доступ к ней [4, с. 18].

При этом следует иметь в виду, что к утечке конфиденциальной информации приводит несанкционированное получение защищаемых сведений как лицами, непосредственно не работающими в организации, так и сотрудниками, не уполномоченными знакомиться с этой информацией.

Нельзя не отметить и тот факт, что конфиденциальное делопроизводство имеет свой специфический объект защиты — конфиденциальный документ. Специфичность конфиденциальных документов по сравнению с документами открытого доступа выражается в особом режиме обращения с ними, налагающем ограничения на ознакомление, копирование и размножение с документами, наличии специальной маркировки, выделяющей эти документы из общего потока, и т. д.

В конфиденциальном делопроизводстве существует и иное отношение к документообороту, который рассматривается не только как технологический процесс (совокупность маршрутов движения документов по установленным пунктам учета, рассмотрения, исполнения и хранения), но и как объект защиты, представляющий собой совокупность (сеть) каналов объективного, санкционированного распространения конфиденциальной документированной информации в процессе управленческой и производственной деятельности пользователей (потребителей этой информации) [7, с. 108].

Важной особенностью конфиденциального делопроизводства является также то, что в силу условий работы с документами ограниченного доступа эта деятельность распространяется и на управленческие, и на научно-технические документы (научно-исследовательские, проектные, конструкторские, технологические и др.).

Соответственно, для работы с ними в организации необходимо разрабатывать специальные правила (инструкции).

Однако независимо от разновидностей конфиденциальных документов необходимо соблюдать общие требования к порядку работы с ними (требования к порядку движения, ознакомления с документами, передачи их в архив и т. п.) и в целом обеспечения сохранности и конфиденциальности защищаемой информации.

Утечка (разглашение), а также утрата конфиденциальной документированной информации обусловлены проявлением различных угроз безопасности конфиденциальных документов, к которым относятся [1]:

1. хищение документа, его части, а также черновиков и проекта документа либо чистого носителя информации, предназначенного для его составления (кража);
2. потеря документа, его чернового варианта, рабочих записей либо чистого носителя (утрата);

3. несанкционированное уничтожение носителя или самой информации (разрушение);
4. подмена документа, его отдельных частей или чистого носителя;
5. несанкционированное копирование информации;
6. несанкционированная модификация (изменение) содержащейся в документе информации и т. д.

Как видно, в конфиденциальном делопроизводстве угрозы включают различные негативные действия, направленные не только на сам документ, но и на черновики и проекты составляемых документов, а также чистые носители, предназначенные для составления документа или его черновика (проекта).

Нередко различные рабочие записи его разработчиков (составителей, исполнителей), возникшие в процессе создания документа, включают еще больший объем конфиденциальных сведений, чем сам документ, и нередко становятся каналом утечки охраняемой информации. Соответственно, уже с момента замысла создания того или иного документа, содержащего конфиденциальные сведения организации, возникает потенциальная угроза утечки (разглашения) этих сведений, в результате чего должны приниматься адекватные меры по ее предотвращению.

В качестве источников угроз конфиденциальной документированной информации могут выступать люди, технические средства обработки и передачи информации, стихийные бедствия и т. д. Способами дестабилизирующего воздействия на защищаемую информацию являются нарушение технологии ее обработки и хранения, физическое воздействие на носитель информации и т. д. [8; с. 69–72].

Кроме того, в силу проявления человеческого фактора могут наблюдаться следующие ситуации:

- в период отсутствия на рабочем месте пользователь не блокирует компьютер, в результате чего доступ к информации имеют посторонние лица;
- при включении компьютера в сеть пользователь не знает, какая информация доступна другим пользователям;
- со своих рабочих компьютеров пользователи выходят в незащищенные сети общего пользования (Интернет), создавая возможность утечки информации;
- пользователи несанкционированно устанавливают на свои компьютеры постороннее программное обеспечение, которое снижает производительность и увеличивает риск выхода из строя системы.

Названные факторы возможны ввиду низкой квалификации или халатности пользователей, недостаточного контроля со стороны администратора безопасности или отсутствия мотивации со стороны руководителя, когда виновные в нарушениях остаются ненаказанными.

Для своевременного реагирования на нарушения необходимо проводить мониторинг безопасности информации, который предполагает постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установления его соответствия требованиям безопасности информации.

Все организации, которые осуществляют обработку конфиденциальной информации (в первую очередь, это персональные данные), должны придерживаться следующих требований:

- выполнять требования Федерального закона за № 152 «О персональных данных»[1], обеспечив при этом все необходимые доказательства законности сбора и обработки персональной информации;
- обеспечивать защиту от несанкционированного распространения персональных данных;

[1] *О персональных* данных: Фед. закон от 27.07.2006 г. № 152-ФЗ (ред. от 23.07.2013 г.) // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). Ст. 3451.

- разрабатывать нормативные локальные акты и техническую организационную документацию для обеспечения регламентированной обработки персональных данных;
- уведомлять управление Роскомнадзора.

Для того чтобы выполнять эти требования, согласно методике ФСКЭМ[1], нужно выполнить следующие работы.

1. Провести изучение процессов сбора и обработки персональной информации в компании. А именно, в каком месте и каком виде они обрабатываются, в каком месте хранятся, кто отвечает за это и имеет к ним доступ, что за источник персональных данных и тому подобные вопросы. Необходимо собрать полную информацию обо всех процессах, связанных с личными данными.
2. Нужно разработать пакет документов, которые относятся к процессу обработки персональных данных, а именно:
   - акт категорирования;
   - концепцию создания системы защиты персональных данных;
   - модель угроз;
   - модель нарушителя;
   - техническое задание на построение системы защиты персональных данных;
   - технический проект (пояснительную записку технического проекта) по построению системы защиты персональных данных;
   - организационно распорядительную документацию.

   В целом количество документов в средней организации составляет около 80 штук, в том числе журналы учета и приказы [2, с. 99–101].
3. Внедрить в организации технические средства защиты согласно разработанной документации.
4. Провести оценку соответствия или же аттестацию информационных систем.

Аттестация и оценка являются специальными установленными документами, благодаря которым организация имеет возможность подтвердить то, что она выполняет все требования действующего законодательства Российской Федерации. Инициатором для разработки такого рода документов выступает Федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК) и Федеральная служба безопасности Российской Федерации (ФСБ). Данные полномочия регламентированы в их нормативно-методических документах и приказах.

Одним из таких документов является приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18.02.2013 г. № 2 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»[2].

Резюмируя вышесказанное, можно заключить, что объем сведений, составляющих конфиденциальную информацию, в конкретной организации определяется руководителями исходя из специфики деятельности организаций. Руководитель вправе самостоятельно устанавливать правила работы с конфиденциальной информацией, в том числе назначать сотрудников, ответственных за учет и хранение конфиденциальных документов, передачу документов в другие подразделения.

---

[1] *Методика* определения актуальных угроз безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) / Утв. заместителем директора ФСТЭК России 14 февраля 2008 г. // СПС Консультант Плюс: [Электронный ресурс]. URL: http://www.consultant.ru/.

[2] *Об утверждении* состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК России от 18.02.2013 г. № 21 / Зарег. в Минюсте России 14.05.2013 г. № 28375 // Российская газета. № 107. 22.05.2013.

Важнейший постулат для документирования конфиденциальной информации заключается в том, что конфиденциальная информация не подлежит разглашению в любом виде и в любой форме и не может стать достоянием третьих лиц.

Организация делопроизводства для конфиденциальных сведений в организации подразумевает наличие разрешительной системы доступа к конфиденциальной информации.

В завершение отметим, что указанная схема является универсальной для документирования конфиденциальной информации. Однако некоторые ее виды — в первую очередь персональные данные — имеют несколько иные принципы документирования, которые определяются исходя из особого административно-правового режима персональных данных. В рамках настоящей статьи раскрыть сущность данных принципов не представляется возможным, однако это актуальная тема для дальнейшей разработки существующей проблематики.

## Литература


1. *Алексенцев А. И.* Конфиденциальное делопроизводство. М.: ЗАО «Интел-Синтез», 2011.
2. *Баймакова И. А.* Обеспечение защиты персональных данных /И. А. Баймакова, А. И. Новиков, А. И. Рогачев, А. Х. Хадыров. М.: 1С-Паблишинг, 2011.
3. *Куняев Н. Н.* Конфиденциальное делопроизводство и защищенный электронный оборот / Н. Н. Куняев, А. С. Демушкин, А. Г. Фабричнов. М.: Двор, 2011. С. 305–306.
4. *Лукашов А. И.* Конфиденциальная информация и коммерческая тайна: правовое регулирование и организация защиты / А. И. Лукашов, Г. Н. Мухин. Мн.: Тесей, 1998.
5. *Магдилова Л. В.* Информационно-правовые нормы Конституции РФ и их развитие в информационном законодательстве // Законы России: опыт, анализ, практика. 2010. № 4.
6. *Некраха А. В.* Организация конфиденциального делопроизводства и защита информации. М.: Проект, 2011.
7. *Степанов Е. А.* Информационная безопасность и защита информации / Е. А. Степанов, И. К. Корнеев. М.: Инфра-М, 2009.
8. *Терещенко Л. К.* Специальные правовые режимы информации // Журнал зарубежного законодательства и сравнительного правоведения. 2011. № 2 (27).


## References


1. Aleksentsev A. I. *Confidential paperwork* [Konfidentsial'noe deloproizvodstvo]. M.: JSC Intel-Sintez [ZAO Intel-Sintez], 2011.
2. Baymakova I. A. *Ensuring protection of personal information* [Obespechenie zashchity personal'nykh dannykh] / I. A. Baymakova, A. I. Novikov, A. I. Rogachyov, A. H. Hadyrov. M.: 1C-Publishing, 2011.
3. Kunyaev N. N. *Confidential paperwork and the protected electronic rotation* [Konfidentsial'noe deloproizvodstvo i zashchishchennyi elektronnyi oborot] / N. N. Kunyaev, A. S. Demushkin, A. G. Fabrichnov. M.: Yard [Dvor], 2011. Pp. 305–306.
4. Lukashov A. I. *Confidential information and trade secret: legal regulation and organization of protection* [Konfidentsial'naya informatsiya i kommercheskaya taina: pravovoe regulirovanie i organizatsiya zashchity] / A. I. Lukashov, G. N. Mukhin. Minsk: Theseus [Tesei], 1998.
5. Magdilova L. V. *Information and legal rules of the Constitution of the Russian Federation and their development in the information legislation* [Informatsionno-pravovye normy Konstitutsii RF i ikh razvitie v informatsionnom zakonodatel'stve ] // Laws of Russia: experience, analysis, practice [Zakony Rossii: opyt, analiz, praktika]. 2010. N 4.
6. Nekrakha A. V. *Organization of confidential office-work and information security* [Organizatsiya konfidentsial'nogo deloproizvodstva i zashchita informatsii]. M.: Project [Proekt], 2011.
7. Stepanov E. A. *Information security and information protection* [Informatsionnaya bezopasnost' i zashchita informatsii] / E. A. Stepanov, I. K. Korneev. M.: Infra-M, 2009.
8. Tereshchenko L. K. *Special legal regimes of information* [Spetsial'nye pravovye rezhimy informatsii] // Journal of the foreign legislation and comparative jurisprudence [Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya]. 2011. N 2 (27).