

gaudeamus

А.В. Некраха, Г.А. Шевцова

Учебное
пособие

**ОРГАНИЗАЦИЯ
КОНФИДЕНЦИАЛЬНОГО
ДЕЛОПРОИЗВОДСТВА
И ЗАЩИТА
ИНФОРМАЦИИ**





УДК 651
ББК 65.050.2
Н48

Рецензенты:

канд. техн. наук *В.А. Граник*;
канд. техн. наук *М.В. Мецатунян*

Н48 Некраха, А.В. Организация конфиденциального делопроизводства и защита информации : учебное пособие / А.В. Некраха, Г.А. Шевцова. — М. : Академический Проект, 2007. — 224 с. — (Gaudeamus).

ISBN 978-5-8291-0844-1 (Академический Проект)

В работе изложена организация конфиденциального делопроизводства и связанные с этим вопросы защиты коммерческой и служебной тайны в государственных и негосударственных организациях.

Рекомендовано в качестве учебного пособия для высших и средних специальных учебных заведений по соответствующим специальностям (специализациям), а также при подготовке и повышении квалификации специалистов по защите информации.

УДК 651
ББК 65.050.2

ISBN 978-5-8291-0844-1

© Некраха А.В., Шевцова Г.А., 2007
© Оригинал-макет, оформление.
Академический Проект, 2007

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ..... 5

Глава I

ПОНЯТИЕ О КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТАХ 6

Глава II

ОРГАНИЗАЦИЯ КОНФИДЕНЦИАЛЬНОГО ДЕЛОПРОИЗВОДСТВА ... 15

Глава III

ПЕРЕЧНИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
И ДОКУМЕНТОВ 25

Глава IV

СИСТЕМА ДОСТУПА
К КОНФИДЕНЦИАЛЬНЫМ ДОКУМЕНТАМ 35

Глава V

УЧЕТ НОСИТЕЛЕЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ... 42

Глава VI

УЧЕТ ИЗДАВАЕМЫХ КОНФИДЕНЦИАЛЬНЫХ
ДОКУМЕНТОВ 50

Глава VII

ПОЛУЧЕНИЕ (ОТПРАВЛЕНИЕ)
КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ И ИХ УЧЕТ 61

Глава VIII

УЧЕТ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ
ВЫДЕЛЕННОГО ХРАНЕНИЯ 71

Глава IX

УЧЕТ КОПИРОВАНИЯ КОНФИДЕНЦИАЛЬНЫХ
ДОКУМЕНТОВ 76

Глава X

ОРГАНИЗАЦИЯ ИСПОЛНЕНИЯ
КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ 82

Глава XI	ФОРМИРОВАНИЕ КОНФИДЕНЦИАЛЬНЫХ ДЕЛ	88
Глава XII	ПОДГОТОВКА КОНФИДЕНЦИАЛЬНЫХ ДЕЛ И ДОКУМЕНТОВ ДЛЯ АРХИВНОГО ХРАНЕНИЯ ИЛИ УНИЧТОЖЕНИЯ	101
Глава XIII	РЕЖИМ СОХРАННОСТИ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ	110
Глава XIV	КОНТРОЛЬ НАЛИЧИЯ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ ...	121
Глава XV	ПРОВЕДЕНИЕ КОНФИДЕНЦИАЛЬНЫХ СОВЕЩАНИЙ	137
Глава XVI	ПРОВЕДЕНИЕ ВНУТРЕННИХ РАССЛЕДОВАНИЙ ПО ФАКТАМ УТРАТЫ (РАЗГЛАШЕНИЯ) КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ	147
Глава XVII	ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА	154
	ПРИЛОЖЕНИЯ	159

■ ПРЕДИСЛОВИЕ

В данной книге на основе требований к защите коммерческой и служебной тайны раскрыты вопросы, связанные с созданием и обработкой конфиденциальных документов, изложены подходы к организации системы доступа к этим документам (информации).

Структура книги отражает последовательность работы с конфиденциальными документами. Изложенные в книге положения базируются на рациональной технологии делопроизводства, оптимизации видов учета и минимизации состава учетных форм документов, соблюдении персональной ответственности за сохранность документов и обеспечение конфиденциальности содержащейся в них информации на всех этапах обращения с документами.

Книга развивается на современном методологическом уровне положения, обоснованные в работах профессора Российского государственного гуманитарного университета А.И. Алексанцева. Вместе с тем она базируется на действующих в настоящее время законодательных и нормативных документах, обобщает практику работы с конфиденциальными документами.

В приложениях изложены основные законодательные и нормативные документы по рассматриваемым вопросам, а также даны рекомендации по учетным формам и оформлению конфиденциальных документов.

Книга рассчитана как на сотрудников подразделений конфиденциального делопроизводства, так и на исполнителей (пользователей) конфиденциальных документов. Полезна она и для руководителей коммерческих организаций (служб безопасности), организующих эффективное и информационно-безопасное обращение с конфиденциальными документами в своей организации.

Учитывая, что в книге систематизировано излагаются все вопросы организации и технологии обращения с конфиденциальными документами, она рекомендуется в качестве учебного пособия в высших и средних специальных учебных заведениях по соответствующим специальностям (специализациям), а также при подготовке и повышении квалификации специалистов по защите информации.

Глава I

ПОНЯТИЕ О КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТАХ

Федеральный закон «Об информации, информационных технологиях и о защите информации» (см. Приложение 1) предусматривает установление для определенной информации ограничения на ее предоставление или распространение. Таковую информацию (информацию ограниченного доступа) составляет информация, отнесенная к государственной тайне, а также конфиденциальная информация, ограничение на доступ к которой устанавливается федеральными законами.

Документированная информация ограниченного доступа, в свою очередь, по условиям ее правового режима, подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

Понятие государственной тайны и связанные с ней степени секретности сведений и грифы секретности носителей этой информации, в соответствии с Федеральным законом «О государственной тайне», распространяются на конкретный перечень сведений в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Ко всем остальным сведениям эти понятия неприменимы.

Под конфиденциальной информацией понимается документированная информация, доступ к которой ограничивается в соответствии с федеральными законами Российской Федерации. Указом Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера»¹ определены следующие виды сведений конфиденциального характера.

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющих идентифицировать его личность (персональные данные).
2. Сведения, составляющие тайну следствия и судопроизводства.
3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).
4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.).
5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).
6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Такое распределение сведений, безусловно, носит общий характер и требует уточнения как в методологическом, так и правовом аспектах.

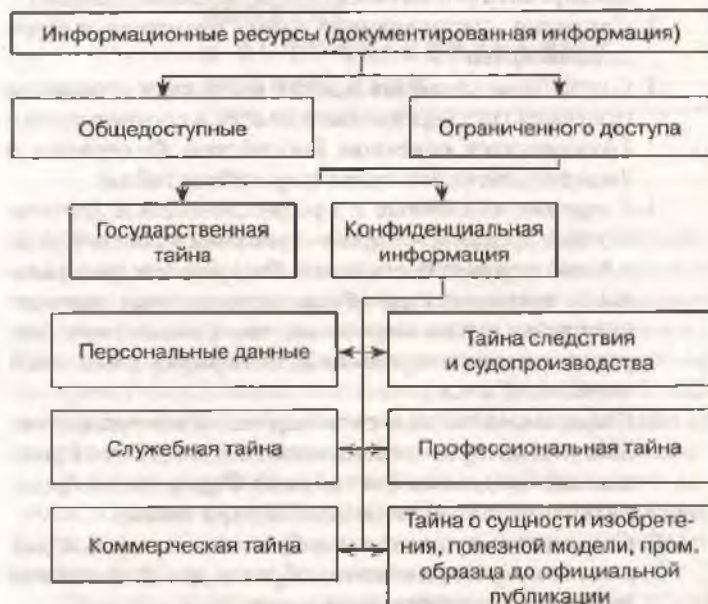
Виды информационных ресурсов по категориям доступа показаны на схеме 1.

Рассмотрим подробнее наиболее распространенные и близкие по смыслу понятия коммерческой и служебной тайны.

С принятием Федерального закона «О коммерческой тайне» (см. Приложение 2) понятие коммерческой тайны получило самостоятельное законодательное закрепление.

Коммерческая тайна прямо связана с коммерческой деятельностью и является необходимым условием ее существования. В современном понимании коммерческая деятельность не привязывается к какой-либо определенной сфере, она охватывает промышленную, торговую, финансовую, научно-исследовательскую и другие виды предпринимательской деятельности.

Виды информационных ресурсов по категориям доступа



В соответствии с законом, коммерческая тайна — конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Непосредственно под информацией, составляющей коммерческую тайну, понимается научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства [ноу-хау]), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

Под режимом коммерческой тайны понимаются правовые, организационные, технические и иные меры, при-

нимаемые владельцем информации, составляющей коммерческую тайну, по охране ее конфиденциальности.

Что касается толкования термина служебной тайны, то кроме определения, данного в упомянутом перечне сведений конфиденциального характера, к служебной информации ограниченного распространения в соответствии с «Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» (см. Приложение 3) относится несекретная информация, касающаяся деятельности государственных организаций, ограничения на распространение которой диктуются служебной необходимостью.

Приведенные определения соответствуют Гражданскому кодексу Российской Федерации. В нем эти виды тайны объединены следующей формулировкой: «Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет доступа на законном основании и владелец информации принимает меры к охране ее конфиденциальности»¹.

Использование (обращение) конфиденциальной информации осуществляется путем ее документирования на различных материальных носителях. Носитель информации — это физическое лицо или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Таким образом, конфиденциальная информация накапливается на различных носителях и защита такой информации во многом сводится к защите ее носителей.

Типы материальных объектов как носителей информации различны и многообразны. Но наиболее массовым типом являются все же носители на бумажной основе, а также хранящие информацию в электронном виде (магнитные носители информации). Соответственно, одним из основных видов защиты документированной конфиденциальной информации является организация специального обращения с указанными носителями. Такая ор-

¹ Статья 139 Гражданского кодекса Российской Федерации.

ганизация (технология) работы с документами называется конфиденциальным делопроизводством.

На документах (носителях), содержащих информацию, относящуюся к служебной или коммерческой тайне, предусмотрено нанесение соответствующих идентификационных реквизитов — грифов. На конфиденциальных документах федеральных органов государственной власти, а также подведомственных им предприятий, учреждений и организаций проставляется гриф (пометка) «Для служебного пользования». На конфиденциальных документах других лиц (физических, юридических) предусмотрено использование грифа «Коммерческая тайна».

К сожалению, информация подвержена различным видам угроз, имеющих свои особенности и последствия. Применительно к конфиденциальной информации эти угрозы могут привести к ее «утрате» или «разглашению».

Термин «разглашение информации» требует особого пояснения, поскольку к открытой информации он не применяется.

В соответствии с основными понятиями, используемыми в Федеральном законе «О коммерческой тайне», разглашение информации, составляющей коммерческую тайну, это: действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации, либо вопреки трудовому или гражданскому договору.

Иными словами, разглашение — это правонарушение (как умышленный, так и неумышленный), т. е. неразрешенный выход такой информации за пределы защищаемой зоны ее функционирования или установленного круга лиц, если этот выход привел к получению информации лицами, не имеющими к ней санкционированного доступа, независимо от того, работают или не работают такие лица в данной организации (на предприятии).

«Утрата» и «разглашение» конфиденциальной документированной информации — понятия собирательные. Они проявляются в различных формах негативного воздействия на информацию, к которым относятся:

- хищение носителя информации или отображенной в нем информации (кража);
- потеря носителя информации (утеря);
- несанкционированное уничтожение носителя информации или записанной в нем информации (разрушение);
- искажение информации (несанкционированное изменение или модификация, подделка, фальсификация);
- блокирование информации (невозможность работать с ней);
- утечка информации (распространение, раскрытие).

В качестве пояснения необходимо отметить, что термин «разрушение» употребляется главным образом применительно к информации на магнитных носителях.

Блокирование информации в данном контексте означает блокирование доступа к ней правомочных пользователей, а не злоумышленников.

К утрате документированной информации приводят хищение и потеря носителей информации, несанкционированное уничтожение носителей информации или только записанной на них информации, искажение и блокирование информации. Утрата может быть полной или частичной, безвозвратной или временной, но в любом случае она наносит ущерб собственнику информации.

Та или иная форма искажения документированной информации может реализоваться в результате преднамеренного или случайного воздействия различными способами на носитель информации или на саму информацию. Источниками таких воздействий могут быть люди, технические средства хранения, обработки и передачи информации, средства связи, техногенные явления и др. Своевременно обнаружить такое искажение и его причину иногда достаточно сложно.

Способами отрицательного воздействия на информацию являются ее неправомерное (несанкционированное, неучтенное) копирование, записывание, передача, съем, а также заражение программ обработки информации компьютерными вирусами, нарушение технологии обработки и хранения информации, вывод (выход) из строя или

нарушение режима работы технических средств обработки и передачи информации, физическое воздействие на носители информации и др.

Разглашение может произойти в результате потери или хищения носителя конфиденциальной документированной информации, а также хищения записанной на нем информации при сохранности носителя. Потерянный носитель не обязательно предполагает разглашение конфиденциальной информации, а хищение конфиденциальной документированной информации также не всегда связано с получением ее лицами, не имеющими к ней доступа.

Но в любом случае утрата в виде потери или хищения конфиденциальной информации если и не приводит к ее разглашению, то всегда создает угрозу такого разглашения. Сложность состоит в том, что зачастую невозможно определить сам факт разглашения (хищения) конфиденциальной информации при сохранности носителя информации.

Необходимо уделять одинаковое внимание предотвращению как утраты защищаемой документированной информации, так и ее разглашения, поскольку ущерб собственности информации грозит в любом случае.

Защита конфиденциальной документированной информации от утраты и разглашения осуществляется в определенной мере в рамках самой организации конфиденциального делопроизводства. Однако защитные мероприятия охватывают и другие объекты, так или иначе связанные с защищаемыми документами (помещения, технические средства обработки и передачи информации и др.).

Порядок обращения с конфиденциальной информацией в отличие от порядка обращения с государственной тайной не имеет строгого нормативного закрепления, хотя сам такой порядок (режим) является необходимым условием ее защиты.

В общем случае для организации работы по охране конфиденциальной информации необходимо осуществление комплекса мер, включающих:

- определение (и периодическое уточнение) конкретного перечня информации, относящейся к конфиденциальной;

- ограничение доступа к информации, относящейся к конфиденциальной, путем установления порядка обращения с такой информацией и контроля за соблюдением такого порядка;
- учет лиц, получивших доступ к информации, относящейся к конфиденциальной, и лиц, которым такая информация предоставлена или передана;
- регулирование отношений по использованию информации, относящейся к конфиденциальной, с работниками на основании трудовых договоров (специальных соглашений) и контрагентами на основании гражданско-правовых договоров;
- введение определенного внутриобъектового и других видов режима, обеспечивающего защиту информации, относящейся к конфиденциальной;
- применение средств и методов технической защиты информации, относящейся к конфиденциальной;
- соответствующее оформление материальных носителей информации, относящейся к конфиденциальной (нанесение грифа и идентификационных реквизитов).

Каждая из этих мер имеет ряд конкретных организационных (управленческих, ограничительных) аспектов, таких как:

- наличие в руководящих документах организации (предприятия), договорах, заключаемых с работниками, в должностных инструкциях положений и обязательств по защите конфиденциальной информации;
- формирование и регламентация деятельности структурного подразделения (должностных лиц) организации (предприятия) по работе с конфиденциальной информацией, обеспечение этого подразделения нормативно-методическими документами по организации и технологии защиты информации;
- построение технологии документирования — составления, оформления, изготовления и издания конфиденциальных документов;
- построение технологии обработки и хранения конфиденциальных документов;

- регламентация порядка и правил работы персонала с конфиденциальной информацией;
- регламентация порядка защиты информации при ведении переговоров, проведении совещаний по конфиденциальным вопросам, приеме посетителей, осуществлении рекламной, выставочной и другой деятельности;
- оборудование и аттестация помещений и рабочих зон, выделенных для осуществления конфиденциальной деятельности, их техническое и технологическое оснащение средствами защиты информации и охраны;
- регламентация пропускного режима на территории, в здания и помещения организации (предприятия);
- регламентация системы охраны территории, здания, помещений и оборудования.

Глава II

ОРГАНИЗАЦИЯ КОНФИДЕНЦИАЛЬНОГО ДЕЛОПРОИЗВОДСТВА

В общем виде к документам ограниченного доступа относятся документы, работа с которыми может производиться по специальному разрешению. Такие документы входят в сферу деятельности не одного, а нескольких типов делопроизводства, в зависимости от того, к какому виду тайны относится содержащаяся в документах информация. Документы, содержащие государственную тайну, относятся к сфере секретного делопроизводства. Документы, содержащие персональные данные и различные виды профессиональной тайны, являются предметом соответствующих типов специального делопроизводства.

В настоящей работе рассматриваются вопросы обращения документов, содержащих коммерческую и служебную тайны. Объединение конфиденциальных документов, содержащих коммерческую и служебную тайны, одним делопроизводством обусловлено тем, что эти документы практически полностью идентичны по технологическим процедурам их составления, обработки, обращения, хранения и защиты.

Конфиденциальное делопроизводство, не имеет строгой нормативной регламентации, так как сам режим защиты такой информации устанавливается собственником информационных ресурсов. При этом учитывается специфика деятельности конкретной организации (предприятия), виды угроз (рисков), соотносятся затраты на его организацию с возможным ущербом от потери конфиденциальности информации.

Конфиденциальное делопроизводство следует определять как деятельность, обеспечивающую документирование конфиденциальной информации; организацию работы с конфиденциальными документами и защиту содержащейся в них информации.

При этом под документированием информации понимается процесс подготовки и изготовления документов, под организацией работы с документами — их получение, учет, копирование, прохождение, исполнение, отправ-ление, систематизация, хранение, уничтожение, а также проверка режима их обращения.

Конфиденциальное делопроизводство в целом базируется на тех же принципах, что и открытое делопроизводство, но в то же время имеет отличия, обусловленные конфиденциальностью документированной информации.

Конфиденциальное делопроизводство распространяется как на управленческую, так и на различные виды производственной деятельности и включает в себя не только работу с готовыми (подписанными, зарегистрированными и т. д.) документами, но и их проектами, рабочими записями, черновиками. Главным в данном случае является содержание в них информации, подлежащей защите.

Соответственно, конфиденциальное делопроизводство отличается от открытого не только большим количеством видов работ, содержанием и технологией их выполнения, а также и обязательной защитой содержащейся в конфиденциальных документах информации.

Конфиденциальное делопроизводство в отличие от открытого должно решать две задачи.

1. Документационное обеспечение всех видов конфиденциальной деятельности.
2. Защиту документированной информации, образующейся в процессе конфиденциальной деятельности.

Первая задача имеет своей целью бесперебойное обеспечение любого вида управленческой и производственной деятельности полной, своевременной и достоверной документированной информацией, а также организацию исполнения и использования документов.

Полноту документированной информации характеризует ее объем, который, с одной стороны, должен быть достаточным для принятия управленческих решений и выполнения производственных заданий, с другой стороны, являться действительно необходимым, не содержащим избыточной, ненужной для деятельности организации (предприятия) информации.

Достоверность документированной информации заключается в ее соответствии объективному состоянию того или другого вопроса, а также в ее юридической силе (правильности оформления соответствующих реквизитов).

Своевременность документированной информации означает, что за время обработки и передачи информации не изменилось состояние вопроса, к которому она относится.

Организация исполнения документов включает в себя и оперативное доведение их до исполнителей, и обеспечение контроля за своевременным исполнением этих документов.

Организация использования документов состоит в обеспечении как текущего (оперативного), так и последующего (ретроспективного) использования документированной информации.

Вторая задача имеет своей целью обеспечение сохранности и конфиденциальности документированной информации, что требует создания и поддержания специальных условий обращения таких документов, гарантирующих надежную защиту как самих документов, так и содержащихся в них сведений.

Сущность конфиденциального делопроизводства обуславливает его организационные и технологические особенности, к числу основных из которых относятся:

- письменное нормативное закрепление общей технологии документирования, организации работы с документами и их защиты;
- регламентирование состава содержащейся в издаваемых документах конфиденциальной информации, в том числе на стадии черновиков (рабочих записей) и подготовки проектов документов;
- обязательный поэкземплярный и полистный учет всех без исключения документов, проектов и черновиков;
- максимально необходимая полнота регистрационных данных о каждом документе;
- фиксация прохождения и местонахождения каждого документа;
- проведение систематических проверок наличия документов;

- разрешительная система доступа к документам и делам, обеспечивающая правомерное и санкционированное ознакомление с ними;
- жесткие требования к условиям хранения документов и обращения с ними, которые должны обеспечивать сохранность и конфиденциальность документированной информации;
- регламентация обязанностей лиц, допущенных к работе с конфиденциальной документированной информацией по ее защите;
- персональная ответственность должностных лиц за учет, сохранность документов и порядок обращения с ними.

Особенностью конфиденциального делопроизводства является и своеобразное переплетение некоторых функций, которые, на первый взгляд, как бы исключают друг друга. В частности, функцией по реализации задачи документационного обеспечения конфиденциальной деятельности является предоставление каждому пользователю документов, необходимых и достаточных для выполнения должностных обязанностей. При этом функцией по реализации задачи защиты конфиденциальной информации будет предотвращение излишнего, необоснованного ознакомления с конфиденциальными документами.

Это означает, что конфиденциальная деятельность должна обеспечиваться минимальным количеством документов при сохранении полноты и достоверности информации, или, другими словами, — предоставление пользователям всех необходимых документов, но только тех, которые действительно требуются для выполнения должностных обязанностей.

В целом организация конфиденциального делопроизводства включает:

- создание подразделения, обеспечивающего изготовление, учет, хранение, обработку и использование конфиденциальных документов, установление его статуса, структуры, численного и должностного состава;
- разработку положения о подразделении и должностных инструкций сотрудников;

- построение технологии документирования: разработки, оформления, изготовления и издания конфиденциальных документов;
- построение технологий обработки, хранения и уничтожения конфиденциальных документов;
- выделение для работы с конфиденциальными документами специального помещения, его техническое и технологическое оснащение, разработку (приобретение) нормативных документов и методической литературы по организации и ведению конфиденциального делопроизводства;
- создание постоянно действующей экспертной комиссии по вопросам защиты конфиденциальной информации;
- определение порядка доступа сотрудников к служебной или коммерческой тайне, обучение их правилам работы с конфиденциальными документами.

Конфиденциальное делопроизводство в силу меньшего по сравнению с открытым делопроизводством объема документов и в целях обеспечения условий для сохранности и конфиденциальности документов должно быть, как правило, централизованным, т. е. сосредоточенным в едином подразделении. Но независимо от выбранной для условий конкретной организации (предприятия) системы конфиденциального делопроизводства (централизованной, децентрализованной, смешанной) необходимо обеспечить методическое единство в построении учета, прохождения и обращения документов.

Подразделение конфиденциального делопроизводства может быть самостоятельным структурным подразделением, подчиненным непосредственно руководителю организации (предприятия), или входить в состав других подразделений, как правило, осуществляющих защиту конфиденциальной информации: службу безопасности, службу защиты информации и др.

В отдельных случаях конфиденциальное делопроизводство может быть возложено на структурное подразделение, которому поручены прием и учет (обработка) открытой документации. Однако это целесообразно лишь при незначительном объеме конфиденциальных документов и в любом

случае требует выделения этого участка работы в отдельный, с предъявлением к нему (и персоналу, выполняющему обязанности на этом участке) специальных требований.

Наименование подразделения конфиденциального делопроизводства, его статус и структуру определяет руководитель организации (предприятия), исходя из объема конфиденциального документооборота и общей структуры организации (предприятия).

Подразделение конфиденциального делопроизводства является составной частью системы защиты коммерческой или служебной тайны, органом, осуществляющим, координирующим и контролирующим работу с конфиденциальными документами. Оно должно рассматриваться как структурное подразделение, непосредственно участвующее в основной деятельности организации (предприятия).

При незначительном объеме конфиденциального документооборота специальное подразделение конфиденциального делопроизводства может не создаваться. В этом случае издание, обработка и хранение конфиденциальных документов возлагается на специально назначенных приказом руководителя организации (предприятия) сотрудников (не менее двух) одного из профильных подразделений (службы безопасности, секретариата). На этих лиц распространяются все задачи, функции, права и ответственность, указанные для подразделения конфиденциального делопроизводства.

Следует подчеркнуть, что в целях более надежного обеспечения сохранности и конфиденциальности документов на подразделение конфиденциального делопроизводства или на специально выделенных для ведения конфиденциального делопроизводства сотрудников должны быть возложены все операции по изготовлению, учету, копированию, хранению, передаче, отправке, систематизации, проверке наличия и уничтожению конфиденциальных документов. Функции исполнителей и пользователей конфиденциальных документов в сфере изготовления и обработки документов ограничиваются разработкой документов и их исполнением. Допустимо и изготовление документов исполнителями, если оно осуществляется в специально предназначенном для этого помещении подразделения конфиденциального делопроизводства под контролем сотрудников этого подразделения.

Технология выполнения работ по обращению конфиденциальных документов складывается из описания содержания работ и последовательности их выполнения. Она может закрепляться в инструкции по конфиденциальному делопроизводству или других документах.

Основные задачи и функции подразделения конфиденциального делопроизводства должны быть закреплены в соответствующем положении, а обязанности, права и ответственность сотрудников этого подразделения или специально назначенных для ведения конфиденциального делопроизводства лиц — в должностных инструкциях. В должностных инструкциях устанавливаются также и квалификационные требования — образование и стаж работы на аналогичной должности.

В соответствии с законодательством сотрудники подразделения конфиденциального делопроизводства несут дисциплинарную, административную и гражданско-правовую ответственность за утрату конфиденциальных документов или разглашение содержащейся в них информации. Поэтому в должностных инструкциях целесообразно указать персональную ответственность сотрудников за сохранность конфиденциальных документов и содержащейся в них информации.

Положение о подразделении конфиденциального делопроизводства и должностные инструкции сотрудников являются организационно-правовыми документами, регламентирующими статус подразделения в целом и каждого из его сотрудников.

При определении задач и функций подразделения конфиденциального делопроизводства необходимо исходить из того, что оно должно не только организовывать и осуществлять документационное обеспечение конфиденциальной управленческой и производственной деятельности организации (предприятия), но и участвовать во всех мероприятиях по предотвращению утраты конфиденциальных документов и разглашения содержащейся в них информации. Это участие не ограничивается разработкой и осуществлением соответствующих мероприятий только в рамках подразделения конфиденциального делопроизводства. Утрата и разглашение конфиденциальной информации в большинстве случаев происходят по вине испол-

нителей и пользователей конфиденциальных документов, нарушающих по разным причинам правила обращения с такими документами. Поэтому значительная часть функций подразделения конфиденциального делопроизводства связана с обучением исполнителей и пользователей правилам работы с конфиденциальными документами и осуществлением контроля за их выполнением.

Этим обусловлены и соответствующие права подразделения конфиденциального делопроизводства, в том числе такие, как участие в подборе кадров для работы с конфиденциальной информацией, внесение предложений об отстранении от такой работы, поощрении или привлечении к ответственности исполнителей и пользователей конфиденциальных документов, участие в проведении внутренних расследований по фактам утраты конфиденциальных документов или разглашения содержащейся в них информации. В целом комплекс задач, функций, прав и ответственности подразделения конфиденциального делопроизводства вытекает из содержания его деятельности.

В особых случаях, когда ценность конфиденциальной информации велика, а, соответственно, ущерб от ее разглашения или утраты критичен для организации (предприятия), назначение сотрудников на соответствующие должности в подразделение конфиденциального делопроизводства целесообразно осуществлять после проведения в отношении них службой безопасности организации (предприятия) специальных проверочных мероприятий (при письменном согласии на это сотрудников и наличии соответствующей лицензии у службы безопасности).

Все сотрудники, принимаемые на работу в подразделение конфиденциального делопроизводства или назначенные для ведения конфиденциального делопроизводства, должны письменно оформить отношения с организацией (предприятием) по соблюдению режима конфиденциальности (см. гл. IV). Сотрудники могут допускаться к работе только после изучения, в части их касающейся, требований действующих нормативно-методических документов по вопросам организации и ведения конфиденциального делопроизводства, обеспечения режима конфиденциальности проводимых работ и проверки знаний этих требований соответствующими должностными лицами.

Подразделение конфиденциального делопроизводства, как уже отмечалось, должно быть обеспечено служебным помещением (при необходимости — несколькими помещениями) для хранения конфиденциальных документов и работы сотрудников подразделения, а также мест для работы исполнителей (пользователей). При этом должно быть исключено несанкционированное (в том числе случайное) ознакомление исполнителей (пользователей) с непредназначенной для них конфиденциальной информацией или вопросами, раскрывающими режим конфиденциальности.

Служебное помещение должно иметь соответствующее технологическое оснащение для выполнения своих функций, быть обеспечено необходимым оборудованием и техническими средствами, включая средства вычислительной техники (ЭВМ), для оперативного изготовления, тиражирования, копирования, обработки документов, надежного их хранения, быстрого поиска. Оснащение служебного помещения должно предусматривать и изготовление необходимых учетных журналов (карточек), бланков документов, приобретение печатей, штампов, а также расходных материалов (бумаги, картриджей, тетрадей и др.).

В служебном помещении необходимо иметь средства противопожарной защиты.

При этом соответствующие технические средства защиты информации должны быть сертифицированы, а помещение в целом должно иметь защиту, предотвращающую намеренное и случайное разглашение (перехват) информации (в том числе по техническим каналам или с использованием технических средств).

Важной составной частью организации конфиденциального делопроизводства является создание в организации (на предприятии) экспертной комиссии по защите конфиденциальной информации. Задачами такой комиссии должны быть:

- разработка перечня информации, составляющей коммерческую или служебную тайну;
- разработка перечней издаваемых организацией (предприятием) конфиденциальных документов;
- разработка системы доступа к конфиденциальным документам;

- снятия грифа конфиденциальности с документов или продление срока его действия;
- экспертиза ценности конфиденциальных документов с целью их отбора для архивного хранения или уничтожения;
- проведение аналитической работы по предотвращению утраты конфиденциальных документов и разглашению содержащейся в них информации;
- другие вопросы, связанные с обеспечением (установлением) режима конфиденциальности.

Учитывая важность задач экспертной комиссии, в ее состав следует включать высококвалифицированных сотрудников, в первую очередь руководителей службы безопасности и конфиденциального делопроизводства, а также руководителей подразделений, имеющих доступ к конфиденциальной информации. Председателем комиссии целесообразно назначать одного из заместителей руководителя организации (предприятия), допущенного ко всем конфиденциальным сведениям.

Такая комиссия создается приказом руководителя организации (предприятия) и должна работать на постоянной основе. Непосредственную работу комиссии организует ее председатель. Задачи, функции и порядок работы комиссии определяются положением о ней.

Глава III

ПЕРЕЧНИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ДОКУМЕНТОВ

Одним из первоочередных и обязательных моментов в организации обращения конфиденциальных документов является определение перечня информации, составляющей коммерческую или служебную тайну. Только определившись с тем, к какой информации надлежит ограничить доступ, можно выстраивать (регламентировать) порядок ее обращения и защиты.

Особо отметим, что необходимо иметь не только перечень информации, относящейся к конфиденциальной, но и обоснование, что эта информация действительно подпадает под определение коммерческой или служебной тайны, иначе перечень может быть признан неправомерным (в судебном порядке).

Рассмотрим технологию разработки такого перечня на примере сведений, составляющих коммерческую тайну. Этот перечень разрабатывается самой организацией (предприятием) — обладателем информации, поскольку состав и объем сведений, составляющих коммерческую тайну, определяется собственником информации. Никто другой не может указывать, какие сведения относить или не относить к коммерческой тайне (за исключением сведений, которые не могут быть отнесены к коммерческой тайне по закону).

Разработкой перечня информации, составляющего коммерческую тайну, должна заниматься экспертная комиссия совместно со службой безопасности.

На первом этапе работы на основе анализа задач, функций и направлений деятельности организации (предприятия) необходимо установить весь состав циркулирующей информации, отображенной на любом носителе, любым

способом и в любом виде. Кроме того, с учетом перспектив развития взаимоотношений с партнерами определить характер дополнительной информации, которая может возникнуть в дальнейшей деятельности. Эта информация классифицируется по тематическому признаку.

На втором этапе определяется, какая из установленной информации должна быть конфиденциальной и отнесена к коммерческой тайне.

Базовым критерием при этом является возможность получения преимуществ от использования информации за счет неизвестности ее третьим лицам. Этот критерий имеет две составляющие: неизвестность информации третьим лицам и получение преимуществ в силу этой неизвестности. Данные составляющие взаимосвязаны и взаимообусловлены, поскольку, с одной стороны, неизвестность информации третьим лицам сама по себе ничего не значит, если не обеспечивает преимуществ, с другой — преимущества можно получить только за счет такой неизвестности. Конфиденциальность является правовой формой и одновременно инструментом обеспечения неизвестности информации.

Названный критерий является объективным показателем возможности отнесения информации к коммерческой тайне, придания информации статуса конфиденциальной. Но это не означает, что при его наличии информация во всех случаях может быть отнесена к коммерческой тайне. Законодательством введены два ограничения на отнесение информации к коммерческой тайне.

Первое ограничение состоит в том, что к коммерческой тайне не может быть отнесена информация, составляющая государственную тайну.

Второе ограничение заключается в том, что к коммерческой тайне нельзя относить информацию, которая должна быть общедоступной в целях предупреждения сокрытия правонарушений и предотвращения нанесения ущерба законным интересам государства, физических или юридических лиц. Перечни такой информации содержатся в законах «Об информации, информационных технологиях и о защите информации» и «О коммерческой тайне». Эти перечни в значительной мере дублируют друг друга (но имеют различную правовую основу) и обязательны к исполнению.

Запрещение относить к коммерческой тайне ту или иную информацию не означает, что всю ее может получить любое юридическое или физическое лицо. Часть ее, затрагивающая законные интересы этих лиц, безусловно, должна им предоставляться, а часть — лишь соответствующим органам власти, наделенным правом контроля такой информации.

Есть и третье ограничение, диктуемое здравым смыслом. Оно состоит в том, что при отнесении информации к коммерческой тайне необходимо учитывать затраты на ее защиту. Если эти затраты превышают ущерб от ее возможного разглашения, то придание информации статуса конфиденциальной теряет смысл.

Следует иметь в виду, что в перечень сведений, составляющих коммерческую тайну, может включаться не только информация, создаваемая в данной организации (на предприятии), но и информация, полученная без использования неправомερных средств¹ при проведении исследований по собственной инициативе, в результате систематических наблюдений и сбора сведений. Такая информация считается полученной правоммерно и самостоятельно независимо от того, что ее содержание может совпадать с содержанием коммерческой тайны другого юридического или физического лица. Кроме того, правоммерно полученной считается конфиденциальная информация, полученная от ее обладателя на основании договора или в результате правопреемства. Организация (предприятие), правоммерно и самостоятельно получившая информацию, одновременно являющуюся коммерческой тайной другого юридического или физического лица, становится обладателем этой коммерческой тайны со всеми предусмотренными законодательством правами.

После установления состава конфиденциальной информации может определяться и дополнительное огра-

¹ К неправомерным средствам (способам) получения информации, составляющей коммерческую тайну, относятся: собиpание информации посредством похищения документов, подкупа или угроз, дачи взятки, введения в заблуждение, нарушения или подстрекательства (принуждения) к нарушению обязательств о соблюдении режима коммерческой тайны, а равно иные незаконные способы (без согласия обладателя коммерческой тайны на ее передачу третьим лицам).

ничение доступа к ней. Действительно, довольно часто бывает необходимо выделить наиболее значимую информацию (из всей конфиденциальной информации) с целью установления для нее более жесткого режима защиты. Чем больше предполагаемый ущерб от ее разглашения, тем ограниченнее должен быть круг лиц, к ней допущенных.

Дополнительное ограничение доступа целесообразно указывать для конкретного документа, например введением, при его адресовании, дополнительной надписи «Только...». Порядок использования этого ограничения, перечень должностных лиц, имеющих право его устанавливать, а также указание о запрещении дальнейшего расширительного адресования документа с такой надписью следует изложить в положении, регламентирующем общую систему доступа (см. гл. IV и Приложение б).

Введение дополнительного ограничения доступа к документу связано с тем, что Федеральным законом «О коммерческой тайне» не предусмотрены степени (грифы) конфиденциальности. Это оправдано, т. к. все вопросы отнесения информации к конфиденциальной и установления режима коммерческой тайны определяются собственниками информации, которые могут иметь разные подходы к определению степени конфиденциальности однотипной информации. В этом случае при рассмотрении в судебном порядке дел о неправомерном получении информации, отнесенной к коммерческой тайне, сложно определить, кто из собственников установил правильную степень конфиденциальности, т. к. критерии отнесения информации к той или другой степени конфиденциальности выбирает сам собственник.

Следующий этап — определение конкретных сроков конфиденциальности информации либо обстоятельств и событий, при наступлении которых конфиденциальность снимается. Продолжительность конфиденциальности информации должна соответствовать срокам действия условий, необходимых и достаточных для признания данной информации конфиденциальной в соответствии с законодательством.

Результаты работы оформляются документально — перечнем информации, составляющей коммерческую тайну, который может иметь следующую форму.

Перечень конфиденциальной информации и документов

Перечень информации, составляющей коммерческую тайну

(наименование организации)

№ п/п	Наименование сведений, относящихся к конфиденциальным	Должностные лица (подразделения), имеющие право распоряжения сведениями	Срок конфиденциальности
1	2	3	4

При значительном объеме конфиденциальных сведений они классифицируются в перечне по разделам, соответствующим сферам деятельности.

Перечень рассматривается экспертной комиссией с оформлением соответствующего протокола, подписывается ее председателем (или на основании протокола — начальником службы безопасности, заместителем руководителя по безопасности) и утверждается (вводится в действие) приказом или распоряжением руководителя организации (предприятия).

В приказе должны быть определены мероприятия по обеспечению функционирования перечня и контролю его выполнения. С приказом и перечнем необходимо ознакомить под роспись всех сотрудников, работающих с конфиденциальной информацией. Копии перечня или выписки из него должны быть направлены конфидентам данной коммерческой тайны. Ими являются физические или юридические лица, которым в силу служебного положения, договора либо на ином законном основании известна коммерческая тайна ее обладателя.

Дополнения и изменения состава включенных в перечень сведений осуществляются таким же порядком. При существенном изменении состава сведений перечень должен составляться заново. Об изменениях в составе коммерческой тайны обладатель информации обязан в письменной форме известить конфидентов данной информации.

Что касается состава информации, являющейся служебной тайной, то в «Положении о порядке обращения со служебной информацией ограниченного распространения» сказано, что руководитель федерального органа

исполнительной власти в пределах своей компетенции определяет категории должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения, а эти лица несут персональную ответственность за обоснованность такого отнесения.

На практике используются обычно два варианта определения состава такой информации. В первом варианте федеральные органы исполнительной власти разрабатывают единые для отрасли перечни сведений ограниченного распространения и направляют их на подведомственные предприятия, в учреждения и организации. Во втором варианте полномочия по разработке перечней передаются руководителям подведомственных организаций (предприятий) и перечни разрабатываются применительно к каждой конкретной организации (производству). Иногда используется и третий, комбинированный вариант, при котором перечни по укрупненной тематике разрабатывают вышестоящие органы, а на основе этих перечней — подведомственные организации (предприятия).

Технология разработки перечня информации, составляющей служебную тайну, и его форма — аналогичны рассмотренным для информации, составляющей коммерческую тайну.

Служебная тайна может быть в любой области деятельности органа власти или предприятия, однако в упомянутом положении также определен состав сведений, которые не могут быть отнесены к служебной информации ограниченного распространения.

Информация, составляющая служебную тайну, по степеням конфиденциальности также не подразделяется. Поэтому дополнительные ограничения в доступе к документам, содержащим служебную тайну, могут быть установлены тем же порядком, что и для коммерческой тайны.

Перечни информации, составляющей коммерческую или служебную тайну, раскрывают тематическое содержание включенных в них сведений. Но эти сведения, как уже отмечалось, фиксируются на различных носителях и могут быть как документированными, так и не документированными.

Документирование конфиденциальной информации является важнейшей составной частью конфиденциального делопроизводства, поскольку от количества, состава и

правильности оформления документов зависят качество и эффективность управленческой и производственной деятельности, достоверность и юридическая сила документов, трудоемкость их обработки. Объем и характер создаваемых документов влияют и на организацию работы по их защите.

Как уже отмечалось, одной из особенностей конфиденциального делопроизводства является регламентирование состава издаваемых документов. Обусловлено это тем, что документ является потенциальным источником разглашения содержащейся в нем информации. Поэтому конфиденциальные документы должны издаваться только при действительной необходимости в письменном удостоверении управленческих, производственных и иных действий. При этом решение задач конфиденциальной деятельности должно обеспечиваться минимальным количеством документов при сохранении полноты необходимой информации.

Установление состава издаваемых конфиденциальных документов направлено не только на предотвращение необоснованного их издания, но и на исключение избыточной конфиденциальной информации в них, определение количества их экземпляров, адресатов, которым они должны направляться, т. к. не вызванная действительной необходимостью рассылка конфиденциальных документов также может привести к разглашению информации. На стадии определения состава издаваемых документов решается вопрос и о придании им необходимой юридической силы путем установления должностных лиц, которые должны согласовывать, подписывать и утверждать тот или другой документ. В конечном итоге регламентация состава издаваемых конфиденциальных документов преследует цель не только исключения необоснованного, но и неконтролируемого их издания.

Состав документированной конфиденциальной информации зависит от функций организации (предприятия), характера ее деятельности, взаимосвязей с другими юридическими и физическими лицами, порядка разрешения вопросов. Такой состав закрепляется перечнем издаваемых конфиденциальных документов.

Но эти перечни должны разрабатываться на основе и в рамках перечней информации, составляющей коммерческую или служебную тайну. Вызвано это тем, что кон-

фиденциальные сведения могут быть зафиксированы как в документах, так и на других носителях: памяти человека, базе данных ЭВМ, выпускаемой продукции, технологических процессах, физических полях и др. Поэтому только после определения состава всех конфиденциальных сведений можно установить те из них, которые должны документироваться.

Определение состава документируемой информации должно увязываться с решением конкретных задач. В зависимости от назначения документируемой информации определяются конкретные виды документов, в которых эта информация должна быть зафиксирована.

В процессе определения необходимых конфиденциальных документов следует проводить работу по сокращению их количества за счет разработки интегрированных документов, в которые можно включить показатели нескольких документов, в том числе путем замены разовых первичных документов накопительными. Однако объединение документов должно осуществляться с таким расчетом, чтобы в итоге не создавалась возможность необоснованного ознакомления со всем документом лиц, имеющих доступ только к части содержания (показателей) документа.

Виды конфиденциальных документов необходимо устанавливать с учетом оптимального объема содержащейся в них информации, исключая избыточные или дублирующие сведения, поскольку ознакомление с избыточной информацией может нанести ущерб ее собственнику.

Необходимо отметить, что разработка конкретного перечня издаваемых документов целесообразна только для тех из них, которые носят периодический и постоянный характер (приказы, отчеты, технические условия и т. д.). Для разовых документов, появляющихся в деятельности организации (предприятия), или при незначительном объеме издаваемых документов такой перечень не имеет смысла и может не составляться (решение о конфиденциальности конкретного документа принимается на основании перечня информации конфиденциального характера).

После установления состава постоянно разрабатываемых (типовых) документов определяется круг лиц, имеющих право составлять, согласовывать и подписывать

Перечень конфиденциальной информации в документах

(утверждать) тот или иной вид документа, а также адреса-ты, которым данный документ должен направляться.

Перечень издаваемых конфиденциальных документов может иметь следующую форму.

Перечень издаваемых конфиденциальных документов

(наименование организации)

Порядковый номер	Наименование документа	Основание для конфиденциальности	Срок конфиденциальности	Подразделение или должностные лица, ответственные за подготовку	Подразделение или должностные лица, согласующие документ	Должностные лица, утверждающие (подписывающие) документ	Кол-во экземпляров	Адресаты
1	2	3	4	5	6	7	8	9

В качестве пояснения необходимо отметить, что в графе 3 дается ссылка на соответствующий пункт перечня информации, составляющей коммерческую или служебную тайну. Графа 4 также должна увязываться с этим перечнем.

При направлении документов различным организациям (предприятиям), как правило, применяется раздельное адресование, т. е. на каждом экземпляре документа проставляется лишь адресат, которому направляется данный экземпляр. В этом случае при адресовании могут указываться обобщенные наименования, а рассылка осуществляться по отдельному расчету (см. Приложение 6).

Кроме того, данный перечень может быть дополнен графой 10, указывающей периодичность издания документов (отчетов, актов и др.).

Перечень издаваемых документов готовится секретариатом или соответствующим подразделением службы безопасности, рассматривается и оформляется протоколом экспертной комиссии (на перечне должна быть согласующая подпись председателя экспертной комиссии)

и утверждается (вводится в действие) приказом или распоряжением руководителя организации (предприятия).

С перечнями под роспись должны быть ознакомлены все лица, наделенные правом составлять, визировать, подписывать и утверждать соответствующие конфиденциальные документы.

Внесение возможных последующих уточнений или изменений в перечни оформляется тем же порядком.

При изменении перечня информации, составляющей коммерческую и служебную тайну, соответствующие изменения вносятся и в перечни издаваемых конфиденциальных документов. О снятии грифа конфиденциальности с отправленных документов должны быть письменно оповещены все адресаты.

При необходимости издания разовых документов, не включенных в перечни, или дополнительных экземпляров документов, их изготовление может производиться по решению соответствующего руководителя, наделенного правом распоряжаться теми или иными конфиденциальными сведениями (указанной в перечне информации, составляющей коммерческую или служебную тайну). Одновременно определяется целесообразность последующего включения таких документов (дополнительных экземпляров) в перечень издаваемых конфиденциальных документов.

В необходимых случаях рассмотренные перечни сами могут иметь гриф конфиденциальности. Гриф конфиденциальности должен соответствовать совокупной степени конфиденциальности сведений, содержащихся в графах этих перечней. При наличии грифа конфиденциальности перечни регистрируются по журналу учета изданных документов.

СИСТЕМА ДОСТУПА К КОНФИДЕНЦИАЛЬНЫМ ДОКУМЕНТАМ

Конфиденциальные документы являются документами ограниченного доступа (распространения). Это означает, что знакомиться и работать с ними могут только лица, получившие на то соответствующие разрешения. Порядок получения и оформления таких разрешений устанавливается системой доступа к конфиденциальным документам.

Система доступа представляет собой совокупность норм и правил, определяющих, кто из руководителей организации (предприятия) и структурных подразделений, кому из пользователей и с какими категориями конфиденциальных документов может давать разрешение на ознакомление, а также каким образом оформляются такие разрешения в зависимости от вида учета документов.

При разработке системы доступа к конфиденциальным документам необходимо руководствоваться следующими требованиями.

1. Доступ к конфиденциальным документам может предоставляться сотрудникам, письменно оформившим с организацией (предприятием) отношения о неразглашении ставших им известными конфиденциальных сведений (по соответствующему виду тайны). Письменное оформление отношений о неразглашении конфиденциальной информации (соблюдении режима конфиденциальности) является обязательным условием для доступа пользователей к документам в пределах этого вида тайны.
2. Доступ к конфиденциальным документам должен быть обоснованным, т. е. базироваться на служебной необходимости ознакомления с конкретным документом именно данного исполнителя (пользователя).

3. Система доступа должна давать возможность обеспечивать исполнителей (пользователей) всеми необходимыми им в силу служебных обязанностей конфиденциальными документами, но только теми, которые действительно необходимы для выполнения конкретного вида работ.
4. Доступ к конфиденциальным документам должен быть санкционированным, т. е. осуществляться только по соответствующему разрешению уполномоченного на то должностного лица. При этом соответствующее должностное лицо может давать разрешение на ознакомление с конфиденциальными документами только входящими в сферу его деятельности (полномочий, курируемых вопросов) и только установленному кругу лиц.
5. Доступ должен оформляться письменно по каждому конкретному конфиденциальному документу. При необходимости ознакомления пользователя только с частью документа в разрешении на ознакомление должны быть указаны разделы (пункты или страницы), с которыми можно знакомить исполнителя (пользователя).

Исполнители документов и должностные лица, которые визировали, согласовывали, подписывали, утверждали документы, а также лица, указанные в тексте распорядительных документов, допускаются к таким документам без оформления дополнительных разрешений (если они продолжают выполнять те же функциональные обязанности). В первом случае это обусловлено тем, что перечисленные лица в силу своего служебного положения уже получили доступ к документам на стадии их подготовки, во втором — тем, что с поручением, содержащимся в распорядительном документе, исполнитель должен быть ознакомлен в обязательном порядке, чтобы знать, что ему поручено.

Поскольку система доступа к конфиденциальным документам содержит значительное количество правовых положений, а нарушение ее требований, приводящее к разглашению конфиденциальной информации, влечет за собой дисциплинарную, административную, гражданско-правовую, а в некоторых случаях уголовную ответственность, то ее следует закреплять в специальном нормативном документе.

Наиболее целесообразно эти вопросы изложить в общем «Положении о режиме коммерческой (служебной) тайны организации (предприятия)» или другом нормативном документе, регламентирующем действия сотрудников, работающих с коммерческой тайной.

Порядок (система) доступа к конфиденциальным документам разрабатывается на основе указанных требований и включает в себя следующие разделы.

1. Общие положения.
2. Полномочия должностных лиц по разрешению доступа к конфиденциальным документам.
3. Порядок оформления разрешений на доступ к конфиденциальным документам.
4. Другие вопросы, связанные с доступом.

В общих положениях указываются: нормативные документы, на которых базируется система доступа; сфера действия; основные задачи и принципы ее построения; на кого возлагается ответственность и кем осуществляется контроль за выполнение указанных норм. Целесообразно изложить также общие требования по работе с конфиденциальными документами (или дать ссылку на разделы Положения или другие нормативные документы, где эти вопросы изложены); основания и порядок прекращения доступа; санкции к нарушителям установленного порядка обращения с конфиденциальными документами; обязанности администрации и персонала по этим вопросам.

Необходимо иметь в виду, что ответственность за невыполнение требований системы доступа несут как должностные лица, имеющие право давать разрешение на доступ к конфиденциальным документам, так и исполнители (пользователи) конфиденциальных документов. Контроль за выполнением норм системы доступа возлагается на руководителей службы безопасности, подразделения конфиденциального делопроизводства и структурных подразделений (в пределах их полномочий).

В случае необходимости указывается порядок установления дополнительного ограничения доступа для отдельных (содержащих наиболее ценную информацию) конфиденциальных документов. Как уже отмечалось, дополнительное ограничение доступа к документу может устанавливаться на-

несением на него специальной пометки (надписи), например «Только:» или «Лично» в реквизите «адресат». В этом случае определяется порядок использования этого ограничения, перечень должностных лиц, имеющих право его устанавливать, а также дается запрещение дальнейшего расширительного адресования документа с такой надписью (см. Приложение 6).

Во втором разделе необходимо перечислить всех должностных лиц, которые могут давать разрешение на доступ к конфиденциальным документам с указанием, какой категории пользователей и по какому составу документов. Основополагающими подходами при этом должны быть следующие:

- руководитель организации (предприятия) имеет право давать разрешение на доступ ко всем видам конфиденциальных документов всем категориям сотрудников;
- заместители руководителя организации (предприятия) по отдельным направлениям имеют право давать разрешение на доступ к соответствующим конфиденциальным документам всем категориям сотрудников, но в пределах своей сферы деятельности;
- руководителям подразделений дается право разрешать доступ к конфиденциальным документам всем сотрудникам своих подразделений по закрепленной тематике работы подразделений; для осуществления доступа к конфиденциальным документам данного подразделения сотрудников других подразделений необходимо разрешение руководителя или соответствующего заместителя руководителя организации (предприятия);
- первые заместители руководителей, а также должностные лица, временно занимающие ту или иную должность, могут, как правило, разрешать доступ к конфиденциальным документам в объеме всех прав, предусмотренных для замещаемых ими лиц.

В третьем разделе необходимо изложить порядок оформления доступа к конфиденциальным документам, зарегистрированным по различным видам учета. Такое разрешение оформляется: по поступившим и изданным документам — в форме резолюции на документе; по документам, зарегистрированным по учету документов выделенного хра-

нения и делам — в форме резолюции на документе или подписанного соответствующим руководителем списка пользователей на внутренней стороне обложки документа (дела), титульном листе либо в карточке учета выдачи документа.

В четвертом разделе предусматриваются: порядок доступа к конфиденциальным документам лиц, не работающих в данной организации (при выполнении совместных работ); вопросы, связанные с доступом на совещания по конфиденциальным вопросам; организация доступа к изделиям, отнесенным к конфиденциальным и другие вопросы, требующие отдельной регламентации (в зависимости от специфики деятельности).

В этом же разделе целесообразно перечислить должностных лиц, имеющих право давать разрешение на снятие копий с конфиденциальных документов.

Следует иметь в виду, что сотрудники органов государственной и муниципальной власти имеют право на доступ к конфиденциальным документам, но только в случаях, установленных законодательством. Порядок предоставления конфиденциальной информации и учет лиц, которым такая информация была предоставлена (передана), также регламентируется системой доступа. Названные органы обязаны обеспечить защиту полученных ими документов от разглашения содержащейся в них информации. За разглашение или неправомерное использование содержащейся в документах конфиденциальной информации должностные лица несут предусмотренную законодательством ответственность.

Порядок (система) доступа к конфиденциальным документам разрабатывается совместно подразделением конфиденциального делопроизводства, экспертной комиссией и службой безопасности. Нормативный документ с этими требованиями (Положение) утверждается приказом руководителя организации (предприятия), в котором определяются и мероприятия по введению его в действие (порядок доведения до сотрудников, осуществление контроля за его выполнением и др.).

Необходимо иметь в виду, что в «Положение о режиме коммерческой (служебной) тайны организации (предприятия)» включаются только те вопросы, которые затрагивают деятельность должностных лиц и исполнителей, являющихся пользователями системы защиты конфи-

денциальной информации. Этот документ не имеет грифа конфиденциальности и доводится под роспись до всех указанных лиц. Что касается организации деятельности подразделений, обеспечивающих режим коммерческой или служебной тайны (служба безопасности, экспертная комиссия, конфиденциальное делопроизводство и др.), то эти вопросы регулируются отдельными нормативными документами и в общем Положении не включаются.

Как уже отмечалось, доступ сотрудников организации (предприятия) к конфиденциальной информации осуществляется на добровольной основе. Эти отношения устанавливаются при приеме гражданина на работу (если доступ к конфиденциальной информации необходим для выполнения им своих трудовых обязанностей) или уже в ходе трудовых отношений.

При этом необходимо выполнить следующие условия:

- ознакомить работника под роспись с перечнем конфиденциальной информации (по соответствующему виду тайны);
- ознакомить работника под роспись с установленным в организации (на предприятии) режимом (мерами по охране конфиденциальности) соответствующего вида тайны и с мерами ответственности за его нарушение;
- создать работнику необходимые условия для соблюдения им установленного режима (мер по охране конфиденциальности) соответствующего вида тайны.

Со стороны работника предполагается принятие следующих обязательств:

- по соблюдению установленного в организации (на предприятии) режима (мер по охране конфиденциальности) соответствующего вида тайны — в том числе (при необходимости) согласие на проведение в отношении него определенных проверочных мероприятий службой безопасности организации (предприятия), если эта служба имеет соответствующую лицензию на осуществление такой деятельности¹;

¹ См. Закон Российской Федерации «О частной детективной и охранной деятельности в Российской Федерации» (в редакции Федеральных законов от 21 марта 2002 г. № 31-ФЗ, от 10 января 2003 г. № 15-ФЗ и от 6 июня 2005 г. № 59-ФЗ).

- о неразглашении конфиденциальной информации (по соответствующему виду тайны), ставшей ему известной в период выполнения трудовых отношений, и не использовании (без соответствующего разрешения) этой информации в личных целях;
- о неразглашении конфиденциальной информации (по соответствующему виду тайны), ставшей ему известной в период выполнения трудовых отношений, после прекращения трудового договора в течение срока, предусмотренного в специальном соглашении или в течение трех лет после прекращения трудового договора, если такое соглашение не заключалось;
- о возмещении причиненного ущерба, если работник виновен в разглашении конфиденциальной информации (по соответствующему виду тайны), ставшей ему известной в связи с выполнением им трудовых обязанностей (в том числе после прекращения трудового договора, в установленные сроки);
- о возврате при прекращении или расторжении трудового договора всех имеющихся у работника материальных носителей конфиденциальной информации (по соответствующему виду тайны).

Примерная форма соглашения о неразглашении коммерческой тайны приведена в *Приложении 4*.

Согласно Трудовому кодексу в трудовом договоре также могут предусматриваться условия о неразглашении охраняемой законом тайны. В трудовой договор могут быть внесены и условия о полной материальной ответственности работника за разглашение охраняемой законом тайны.

Кроме того, предусмотрена возможность расторжения трудового договора по инициативе работодателя в случае однократного грубого нарушения работником трудовых обязанностей в виде разглашения охраняемой законом тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей.

УЧЕТ НОСИТЕЛЕЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Учет конфиденциальных документов является одной из важнейших составных частей конфиденциального делопроизводства. В открытом делопроизводстве вместо термина «учет» употребляется термин «регистрация», которая представляет собой «запись учетных данных о документе по установленной форме, фиксирующая факт его создания, отправления или получения»¹. Основная цель регистрации — построение поисковой системы по документам.

В конфиденциальном делопроизводстве запись учетных данных о документе не сводится только к фиксации факта его создания, отправления или получения и построению поисковой системы по документам. Важнейшая цель записи учетных данных состоит в обеспечении сохранности конфиденциальных документов и предотвращении, таким образом, разглашения содержащейся в них информации. Для достижения этого в регистрационных формах необходимо фиксировать не только данные о самом документе (включая количество его экземпляров и листов), но и любое движение и местонахождение документа, что позволяет, помимо расширения справочно-поисковых данных о документе, обеспечивать персональную ответственность за его сохранность. Поэтому применительно к конфиденциальным документам употребляется термин «учет», т. к. он является более емким и не сводится только к фиксации данных о реквизитах документа.

Учет документов, содержащих коммерческую или служебную тайну, осуществляется одинаково. Учету подлежат все без исключения изготовленные в организации (на

¹ Типовая инструкция по делопроизводству в федеральных органах исполнительной власти, утвержденная приказом Минкультуры России 2005 г. № 536.

предприятия) и полученные извне конфиденциальные документы.

Конфиденциальные документы можно учитывать в журналах, карточках или автоматизировано (с помощью компьютеров). Если содержащиеся в учетных формах сведения по совокупности являются конфиденциальными, то им должен присваиваться гриф конфиденциальности. Порядок учета журналов (карточек) изложен в гл. XI.

При заполнении учетных форм необходимо предусматривать между строками (по каждой регистрационной записи) достаточно места для последующего внесения информации (отметок) о движении документа (носителя) в соответствующих графах.

Во всех учетных формах (журналах, карточках) не допускаются подчистки и исправления записей, в том числе с применением корректирующей жидкости. Ошибочная запись зачеркивается одной чертой. Вносимые исправления заверяются подписью сотрудника подразделения конфиденциального делопроизводства с проставлением даты.

Учет конфиденциальных документов подразделяется на три вида: поступивших (входящих) документов, изданных документов и документов выделенного хранения.

Учет поступивших (входящих) документов охватывает документы, поступившие от других организаций (предприятий). В некоторых случаях допускается поступившие документы сразу ставить на учет документов выделенного хранения (без присвоения им регистрационного номера по учету поступивших документов).

Учет изданных документов охватывает документы, изготовленные в данной организации (на предприятии) рукописным или машинописным способами (в том числе с использованием компьютеров), независимо от того, направляются эти документы в другие организации (на предприятия) или являются внутренними.

Учет документов выделенного хранения охватывает все документы (поступившие, изданные), не подлежащие подшивке в дела.

Но прежде чем рассмотреть учет названных видов документов, необходимо определиться с требованиями к учету самих носителей конфиденциальной информации, на которых делаются рабочие записи или которые используются в качестве черновиков документов.

Проекты конфиденциальных документов, как и проекты открытых документов, могут печататься:

- с черновика, на котором они составлены;
- с текста, нанесенного на иной носитель информации;
- без использования того и другого (в том числе с голоса, с диктофона).

Черновики и проекты открытых документов не регистрируются, регистрируется уже готовый (утвержденный, подписанный) документ, а его черновик (при наличии) уничтожается исполнителем (составителем) документа без отражения в регистрационных формах факта уничтожения.

Распространение такого порядка на черновики конфиденциальных документов недопустимо, поскольку не гарантирует защиту содержащейся в них информации. Даже когда в учетных формах производится отметка об уничтожении черновика, с которого печатался проект документа, нередко оказывается, что существуют и другие, неучтенные варианты черновиков. Такие варианты не всегда уничтожаются установленным порядком (бумагорезательными техническими средствами), а иногда просто выбрасываются исполнителем или бесконтрольно хранятся для дальнейшего возможного использования. Это может привести к разглашению конфиденциальной информации. Поэтому все носители, предназначенные для составления черновиков (проектов) конфиденциальных документов, следует учитывать предварительно, до внесения в них записей.

Все сказанное в равной степени относится и к отпечатанным проектам конфиденциальных документов независимо от того, с черновика они печатались или без его использования, поскольку может быть несколько вариантов проекта, отдельные листы проекта могут перепечатываться, может меняться и количество экземпляров проекта. Это также создает возможность для разглашения содержащейся в проектах информации (или отдельных ее частей). Следовательно, должны учитываться и проекты конфиденциальных документов на стадии их изготовления.

Учет черновиков и отпечатанных проектов позволяет предотвращать неправомерное обращение с ними и, кро-

ме того, обеспечивает контроль за подготовкой документов, их соответствием перечню издаваемых конфиденциальных документов.

Учет носителей, используемых для составления конфиденциальных документов, осуществляется подразделением конфиденциального делопроизводства.

Самыми распространенными носителями документированной конфиденциальной информации являются бумажные и машинные носители.

Бумажными носителями могут быть:

- для текстовых документов — специальные блокноты, отдельные листы бумаги, типовые формы документов, стенографические и рабочие тетради;
- для чертежно-графических документов — листы ватмана, кальки, миллиметровки.

Специальный блокнот (спецблокнот) предназначен для составления черновиков документов. Он представляет собой сброшюрованные и пронумерованные листы бумаги с линией отрыва и контрольным листом, в котором проставляются номера листов спецблокнота.

Стенографическая тетрадь используется для стенограмм, рабочая тетрадь, как правило, — для различных рабочих и справочных записей, но в ней допускается возможность составлять и черновики документов (особенно больших по объему).

Остальные носители могут использоваться как для составления черновиков, так и для печатания или рукописного изготовления проектов документов. При этом типовые формы документов должны содержать только открытую информацию и иметь в соответствующих местах пропуски для последующего внесения конфиденциальной информации.

Перед постановкой на учет носители должны быть оформлены соответствующим образом.

На обложках спецблокнотов проставляется штампом (или типографским способом) слово «Спецблокнот» и в правом верхнем углу гриф конфиденциальности. Листы спецблокнота должны быть пронумерованы.

На обложках рабочих и стенографических тетрадей указываются вид носителя, гриф конфиденциальности.

фамилия и инициалы исполвителя. Листы тетрадей нумеруются (исполнителем). На обороте последнего листа ставится штамп с указанием в нем количества листов, заверяемого подписью сотрудника подразделения конфиденциального делопроизводства.

Штамп имеет следующую форму.

В данном экземпляре пронумеровано _____
(цифрами)
_____) листов
(прописью)

(подпись должностного лица)
« » _____ 20 г.

Листы типовых форм документов нумеруются (исполнителем), на первом листе проставляется гриф конфиденциальности.

На отдельных листах бумаги, ватмана, миллиметровки, кальки в соответствующих графах основных надписей штампов или других установленных местах исполнителем проставляются:

- на всех носителях — гриф конфиденциальности и номера листов;
- на носителях, предназначенных для чертежно-графических документов, кроме того, — количество листов, подразделение, фамилия и инициалы исполнителя.

На носителе, предназначенном для составления одного конкретного документа, целесообразно указывать наименование этого документа.

Бумажные носители учитываются в журналах или карточках, имеющих следующую форму.

Журнал учета носителей (типовых форм, листов) с грифом _____

Учетный №	Дата регистрации	Вид (назначение)	Кол-во листов	Фамилия и инициалы пользователя	Подпись за получение и дата	Подпись за сдачу и дата	Отметка об уничтожении, отправке, взятии на учет выделенного хранения
1	2	3	4	5	6	7	8

В графе 3 пишется: спецблокнот, листы, типовые формы (конкретно), рабочая тетрадь и др. В необходимых случаях может указываться назначение носителя, например, «для черновиков», «для рабочих записей», «для совещания».

Одновременно на самих носителях проставляется:

- на спецблокнотах:

- в верхнем левом углу лицевой стороны обложки штамп (если не проставлено типографским способом) с указанием учетного номера и количества листов; штамп имеет следующую форму:

Уч. № _____
Кол-во _____
листов _____

- на каждом листе в верхнем левом углу — учетный номер;
- на рабочих и стенографических тетрадях: в верхнем левом углу лицевой стороны обложки (а при невозможности — в верхнем левом углу первой страницы) штамп с указанием учетного номера и количества листов;
- на отдельных листах бумаги, типовых формах документов, ватмана, кальки, миллиметровки:
 - в верхнем левом углу первого листа штамп с указанием учетного номера и количества листов (на каждом листе носителей чертежно-графической информации — только учетного номера);
 - в верхнем левом углу остальных листов штамп с указанием учетного номера; штамп имеет следующую форму:

К уч. № _____

После постановки на учет носитель передается исполнителю с заполнением граф 5 и 6 журнала учета.

При необходимости постановки на учет дополнительных листов носителя (при нехватке ранее взятых листов для составления черновика документа или для замены испорченных листов) они нумеруются от последнего листа ранее учтенного по этому номеру носителя; регистрируются в журнале учета бумажных носителей за тем же номером, что

и ранее взятые листы, отдельной строкой. На каждом листе проставляется штамп с указанием — к какому учетному номеру относится лист, а на первом листе всего носителя прежнее количество листов зачеркивается и проставляется новое с учетом дополнительных листов. Исправление заверяется подписью сотрудника подразделения конфиденциального делопроизводства. Выдача дополнительных листов производится под отдельную роспись в графе 6 журнала учета.

В графе 7 сотрудником конфиденциального делопроизводства проставляется отметка за возврат носителя.

В графе 8 проставляются наименование адресата, которому отправлен носитель, наименование, номер и дата сопроводительного документа, а также наименование, номер и дата сопроводительного документа при возврате носителя (по журналу учета поступивших документов). В этой же графе проставляется учетный номер носителя при переводе его на учет выделенного хранения (например, для чертежно-графических документов).

Если бумажный носитель подлежит уничтожению, то это осуществляется определенным порядком, изложенным в последующих главах.

При уничтожении отдельных листов черновики, спецблокноты, проекты документов в графе 8 журнала учета носителей пишется (или проставляется штампом) слово «Уничтожено». Отметка об уничтожении заверяется подписями двух сотрудников подразделения конфиденциального делопроизводства с проставлением даты уничтожения. При уничтожении рабочих и стенографических тетрадей, документов после слова (штампа) «Уничтожено» указывается номер и дата акта об уничтожении.

Машинные носители информации необходимы при изготовлении проектов документов с помощью средств вычислительной техники (ЭВМ). К ним относятся: жесткие магнитные диски, гибкие магнитные диски (дискеты), магнитные ленты, магнитооптические диски, оптические диски и т. д.

Компьютеры (ЭВМ), используемые для изготовления конфиденциальных документов, учитываются службой безопасности и должны иметь соответствующие виды защиты. Машинные носители, предназначенные для записи (фиксирования) конфиденциальной информации, должны учитываться подразделением конфиденциального делопроизводства.

Учет носителей конфиденциальной информации

производства до нанесения на них информации, в журналах или карточках учета, имеющих следующую форму.

Журнал учета машинных носителей с грифом _____

Учетный № носителя	Дата регистрации	Вид и тип носителя	Фамилия и инициалы пользователя	Подпись за получение и дата	Подпись за сдачу и дата	Наименование информации на носителе или отметка об ее уничтожении (переносе)	Отметка об уничтожении или отправке носителя
1	2	3	4	5	6	7	8

В графе 3 проставляется тип и марка носителя.

В графе 8 проставляется наименование адресата, которому отправлен машинный носитель, номер и дата сопроводительного документа, а также номер и дата сопроводительного документа при возврате носителя (по журналу учета поступивших документов).

Если машинный носитель в силу различных причин уничтожается, то указывается номер и дата акта об уничтожении. На самих машинных носителях проставляются их учетные номера и грифы конфиденциальности (аббревиатурой).

В зависимости от количества и продолжительности хранения носителей учет может осуществляться в пределах года или нескольких лет. В последнем случае учетные номера каждого года продолжают номера предыдущих лет. По окончании непрерывного учета заводится новый учет за новыми номерами. Числящиеся (не уничтоженные) по предыдущему учету носители перерегистрируются по новому учету с отметкой о перерегистрации каждого носителя в предыдущей учетной форме, которая проставляется следующим образом: «Перерегистрирован в журнал за 20__ год под № __» — с указанием года журнала и номера носителя. Отметка проставляется в графе 8 журналов учета носителей.

Листы журналов учета должны быть перед заведением пронумерованы. На обратной стороне последнего листа журнала проставляется штамп с указанием количества листов, заверенный подписью сотрудника конфиденциального делопроизводства.

УЧЕТ ИЗДАВАЕМЫХ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

Последовательность подготовки (издания) конфиденциальных документов показана на схеме 2.

Проекты конфиденциальных документов могут изготавливаться рукописным способом, на пишущей машинке и при помощи средств вычислительной техники (ЭВМ). Рукописным способом допускается готовить отдельные внутренние документы (докладные записки, справки и др.), а также вносить переменную часть в типовые формы документов. Проекты других текстовых документов изготавливаются печатным способом, либо с черновика, либо с другого носителя (включая звуковоспроизводящие устройства), либо под диктовку, либо непосредственно исполнителем. Проекты чертежно-графических документов могут изготавливаться как рукописным способом, так и при помощи печатных устройств.

Печатающие проекты конфиденциальных документов следует осуществлять в специально оборудованных помещениях подразделения конфиденциального делопроизводства или машинописного бюро. Используемые для печатания средства вычислительной техники и электрические пишущие машинки должны быть защищены от возможного перехвата возникающих при их работе электромагнитных излучений.

При любом способе изготовления (рукописном, печатном) проект документа должен иметь все необходимые и правильно оформленные реквизиты. В случае, если документ печатается с черновика, на первом листе черновика должны быть проставлены количество необходимых экземпляров проекта документа и фамилия исполнителя, а если подлежащий изданию документ не предусмотрен перечнями издаваемых конфиденциальных документов,

то на черновике дополнительно должна быть разрешительная надпись руководителя подразделения, имеющего право распоряжения конфиденциальной информацией.

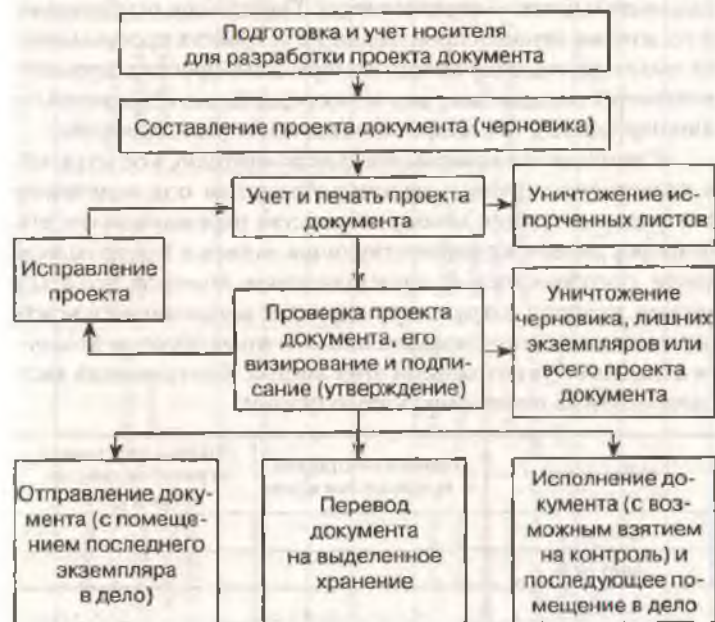
При приеме черновика от исполнителя сотрудник подразделения конфиденциального делопроизводства обязан:

- при составлении черновика в спецблокноте — просчитать количество листов черновика и изъять их из блокнота;
- при составлении черновика на отдельных листах бумаги или в типовой форме документа — просчитать количество его листов;
- при составлении черновика в стенографической или рабочей тетради — проверить соответствие наличия листов тетради указанному количеству.

Если проект печатается с другого документа, то просчитывается количество листов этого документа.

Схема 2

**Последовательность подготовки (издания)
конфиденциального документа**



В предыдущей главе было отмечено, что проекты конфиденциальных документов учитываются на стадии их изготовления. Поэтому после приема черновика сразу производится присвоение учетного номера проекту документа, который будет напечатан с этого носителя. Учетный номер будущего документа проставляется и на черновике, с которого он печатается.

Учетные номера проектов проставляются в журналах (карточках) учета изданных конфиденциальных документов, имеющих форму, представленную на с. 53.

В графе 1 проставляется очередной порядковый номер документа, который будет напечатан с данного носителя, и аббревиатурой гриф конфиденциальности (ДСП или КТ). Все документы (внутренние и подлежащие отправлению) учитываются по единой нарастающей нумерации.

При приеме черновика заполняются графы 1–5. В графе 5 проставляются учетный номер носителя, присвоенный ему по журналу учета носителей, и через дробь номера листов носителя, являющихся черновиком данного документа (при последовательности номеров листов — через тире, при непоследовательности — через запятую). По машинным носителям и носителям звуковоспроизводящих устройств проставляются только их виды и учетные номера. Если проект документа печатается под диктовку или непосредственно исполнителем (без черновика), то в графе пишется «б/ч» (без черновика).

Спецблокнот возвращается исполнителю, а об изъятых в качестве черновиков листах работником подразделения конфиденциального делопроизводства (или машинописного бюро) делается соответствующая запись в контрольном листе спецблокнота (с проставлением номеров изъятых листов, подписи сотрудника и даты). В дальнейшем в контрольном листе спецблокнота аналогичным образом делается отметка об уничтожении этих листов. Контрольный лист спецблокнота имеет следующую форму.

№№ листов	Подпись сотрудника за прием листов и дата	Подпись сотрудника за уничтожение листов и дата
Лист № 1		
Лист № 2		
(и т. д.)		

Журнал учета изданных документов с грифом

Учетный № и гриф конфиденциальности документа	Дата документа	Вид (заголовок) документа	Фамилия и инициалы исполнителя	Уч. № черновика / кол-во листов	Кол-во отпечатанных экземпляров	Кол-во листов в каждом экземпляре	Подпись за получения черновика, отпечатанных документов и дата
1	2	3	4	5	6	7	8
Продолжение							
Отметка об уничтожении порченных листов (подписи и дата)	Отметка о получении и уничтожении черновика (подписи и дата)	Подпись за возврат отпечатанного документа и дата	№№ экземпляров	Куда отправлен документ	С каким документом (за каким №) отправлен (№, дата)	Место хождения (№ дела, №№ листов)	Место хождения (№ по учету выделенного хранения)
9	10	11	12	13	14	15	16

За получение отдельных листов бумаги, типовой формы документа, стенографической или рабочей тетради, документа, с которого должен печататься проект, сотрудник подразделения конфиденциального делопроизводства (машиннописного бюро) выдает разовую расписку (бланки расписок тиражируются) следующей формы.

РАСПИСКА	
Во временное пользование получены от	

<i>(фамилия, инициалы)</i>	
документы за № _____	всего на _____ листах.
« » _____	20 г. _____
<i>(подпись)</i>	

При большом объеме документов разовые расписки могут быть заменены постоянным реестром, выдаваемом исполнителю, с регистрацией и под роспись в журнале учета носителей. Указанный реестр имеет следующую форму.

Реестр учета временно передаваемых документов

Дата	Вид доку- мента	Учетный № и гриф конфи- денциаль- ности	Кол-во листов	Подпись за по- лучение документа и дата	Подпись за возврат документа и дата
1	2	3	4	5	6

При печатании проекта документа на каждом листе каждого экземпляра документа проставляется учетный номер, присвоенный проекту по журналу учета изданных документов. Учетный номер проставляется на первом листе документа (в определенном для этого реквизита месте), на последнем листе в реквизите «Отметка об исполнителе», а также на остальных листах документа (если они есть) в левом нижнем углу лицевой стороны. При этом рядом с номером проставляется аббревиатурой гриф конфиденциальности документа. Порядок нанесения и расположения реквизитов на документах изложен в *Приложении 6*.

Проставление регистрационного номера и грифа конфиденциальности на всех листах изданного конфиденциального документа необходимо для того, чтобы в случаях,

когда документ по каким-либо причинам окажется разрозненным, можно было установить принадлежность отдельных листов к определенному документу и тем самым предупредить случайное уничтожение листов или несанкционированное ознакомление с их содержанием.

После печатания проекта документа заполняются графы 6–7 журнала учета изданных документов. Проект документа вместе с черновиком передается исполнителю под роспись в графе 8. Разовая расписка, выданная ранее исполнителю за получение носителя (черновика), возвращается сотруднику подразделения конфиденциального делопроизводства и уничтожается (или делается соответствующее списание в реестре).

При необходимости перепечатывания отдельных листов проекта документа без изменения общего количества листов от исполнителя принимаются по разовой расписке (или реестру) все экземпляры листов, подлежащие перепечатыванию. Вновь отпечатанные листы передаются исполнителю взамен разовой расписки (или с отметкой в реестре), а испорченные листы уничтожаются установленным порядком с отметкой в графе 9.

При необходимости перепечатывания проекта документа с изменением количества листов перепечатывание производится за новым учетным номером. От исполнителя принимаются правленный и все другие экземпляры проекта, а также черновик с соответствующими отметками в графах 9 и 10 журнала учета изданных документов. Технология учета и выдачи вновь отпечатанного проекта аналогична технологии учета и выдачи первоначального проекта, при этом в графе 5 указывается «С № _____» с проставлением номера перепечатываемого проекта.

При необходимости изготовления дополнительных экземпляров проекта документа в графе 6 журнала учета изданных документов под ранее произведенной записью через знак «+» проставляется количество дополнительных изготовленных экземпляров. Нумерация дополнительных экземпляров проекта производится от последнего номера ранее пронумерованных экземпляров. Роспись за получение таких экземпляров производится отдельно от предыдущей.

При рукописном изготовлении проекта текстового документа на отдельных листах или рукописном заполне-

нии типовой формы документа, а также при разработке чертежно-графических документов носители могут учитываться или по журналу учета бумажных носителей, или сразу по журналу учета изданных документов. В последнем случае в графе 5 пишется слово «Рукопись».

Если проект документа был отпечатан как открытый, а в процессе визирования или подписания было принято решение о переводе его в разряд конфиденциальных, то исполнителем должны быть представлены в подразделение конфиденциального делопроизводства все экземпляры отпечатанного проекта и черновик. На обороте последнего экземпляра проекта исполнитель указывает, сколько экземпляров отпечатано и сколько листов в черновике, заверяя эти данные своей подписью.

При отсутствии черновика или отдельных экземпляров проекта документа принимаются меры по их поиску. Если они не будут найдены, то об этом делается отметка на обороте последнего экземпляра проекта за подписью руководителя подразделения, в котором разрабатывался проект. Об обстоятельствах утраты докладывается руководителю организации (предприятия) для принятия соответствующих решений. Фактически представленные экземпляры проекта документа и черновик регистрируются в журнале учета изданных документов. При этом на черновике проставляется гриф конфиденциальности и учетный номер проекта документа. Проект документа оформляется в соответствии с правилами, предъявляемыми к конфиденциальным документам, и выдается вместе с черновиком (при наличии) исполнителю под роспись в графе 8.

После отработки проекта текстового документа исполнитель должен проставить на экземплярах документа их номера, завизировать последний экземпляр, получить необходимые визы должностных лиц, подписать (утвердить) проект у соответствующего руководителя и передать все экземпляры документа вместе с черновиком (если документ печатался с черновика) в подразделение конфиденциального делопроизводства. Если проект документа по каким-либо причинам не был подписан, то все его экземпляры вместе с черновиком также передаются в подразделение конфиденциального делопроизводства.

Сотрудник подразделения конфиденциального делопроизводства расписывается за получение черновика и документа (проекта) в графах 10 и 11 журнала учета изданных документов.

Черновик, проект (как неподписанный, так и перепечатанный), лишние экземпляры документа уничтожаются установленным порядком. При уничтожении испорченных отпечатанных листов и листов черновика в графах 9 и 10 журнала учета изданных документов пишется слово «Уничтожено» или проставляется штамп следующей формы.

УНИЧТОЖЕНО

При уничтожении проекта документа в графе 11 пишется слово или проставляется штамп «Уничтожено» (при уничтожении лишних экземпляров документа — с указанием их номеров). Отметки об уничтожении заверяются подписями двух сотрудников подразделения конфиденциального делопроизводства с проставлением даты.

В графе 8 журнала учета бумажных носителей производится отметка об уничтожении носителя (кроме спецблокнотов и рабочих тетрадей) в качестве черновика изданного документа (проекта). Отметка оформляется следующим образом: «Уничтожено как черновик № _____» с указанием номера изданного документа (проекта).

Если носитель не являлся черновиком, а уничтожается по каким-либо другим причинам, то в графе 8 журнала учета бумажных носителей пишется слово или проставляется штамп «Уничтожено».

И в первом, и во втором варианте отметка об уничтожении заверяется подписями двух сотрудников подразделения конфиденциального делопроизводства с указанием даты.

Испорченные, не являющиеся черновиком листы спецблокнота, если он предназначен для использования несколькими исполнителями, также должны изыматься (с отметкой об изъятии и уничтожении в контрольном листе спецблокнота). Такой порядок вызван необходимостью исключения необоснованного ознакомления других исполнителей с конфиденциальной информацией, зафиксированной на испорченных листах. Таким же способом испорченные листы могут уничтожаться и при использовании

спецблокнота одним исполнителем. Однако в этом случае допускается уничтожение испорченных листов вместе с обложкой и корешками изъятых листов спецблокнота после использования всех листов.

При уничтожении полностью использованного спецблокнота в контрольном листе проверяется наличие отметок и подписей об изъятии и уничтожении использованных листов. Спецблокнот уничтожается с обложкой, корешками изъятых листов и с испорченными листами (если они не были уничтожены ранее), а в графе 8 журнала учета бумажных носителей пишется слово или проставляется штамп «Уничтожено», заверяемый подписями двух сотрудников подразделения конфиденциального делопроизводства, с указанием даты.

Испорченные листы бумаги, ватмана, кальки, миллиметровки уничтожаются тем же порядком, как и листы черновика.

Листы, отобранные для уничтожения, помещаются в специальную папку, находящуюся в подразделении конфиденциального делопроизводства (машинописного бюро). Содержимое этой специальной папки в последующем уничтожается двумя сотрудниками подразделения конфиденциального делопроизводства путем измельчения бумагорезательными техническими средствами. При этом листы должны быть разрезаны на куски, гарантирующие невозможность восстановления текста. Уничтожение, как правило, должно производиться после проведения проверки наличия конфиденциальных документов за истекший день, что позволяет в случае недостачи каких-либо документов проверить содержимое папки на предмет случайного помещения в нее недостающих документов.

Изготовленный проект чертежно-графического документа дооформляется исполнителем в соответствии с требованиями по оформлению и после подписания соответствующими лицами передается в подразделение конфиденциального делопроизводства с отметкой по месту регистрации: в графе 8 журнала учета бумажных носителей или графе 11 журнала учета изданных документов.

В случае печатания конфиденциальных документов в машинписном бюро отпечатанные проекты документов и их черновики передаются непосредственно в подразде-

ление конфиденциального производства, где их и получает исполнитель. При этом в машинописном бюро графы 10—16 журнала учета изданных документов не заполняются, а передача документов сотруднику подразделения конфиденциального делопроизводства осуществляется под роспись в графе 8.

В подразделении конфиденциального делопроизводства учет полученных документов ведется по такому же журналу.

Если изданный конфиденциальный документ подлежит отправлению с сопроводительным письмом, то оно составляется и оформляется в изложенном выше порядке применительно к текстовым документам, регистрируется за самостоятельным учетным номером, на нем проставляется гриф конфиденциальности, соответствующий грифу конфиденциальности приложения, независимо от того, содержит или нет само сопроводительное письмо конфиденциальную информацию. При наличии нескольких приложений (конфиденциальных и открытых) сопроводительному письму присваивается такой же гриф, как и на конфиденциальном приложении.

Регистрация сопроводительного письма за самостоятельным учетным номером обусловлена тем, что оно, как правило, составляется и печатается не одновременно с приложениями, а позже, тогда как каждому конфиденциальному документу учетный номер присваивается на стадии его печатания. К тому же, с сопроводительным письмом могут быть отправлены документы, зарегистрированные по журналу учета изданных документов и по другим видам учета.

Необходимость проставления на сопроводительном письме грифа конфиденциальности вызвана тем обстоятельством, что без соблюдения этого требования подавляющее большинство сопроводительных писем будут не конфиденциальными, а открытыми, но поскольку документы отправляются за номерами сопроводительных писем, то формально и конфиденциальные приложения окажутся открытыми, со всеми вытекающими последствиями для их сохранности и конфиденциальности.

Подразделение конфиденциального делопроизводства наряду с руководителями соответствующих подразделений должно осуществлять контроль за соответствием

документов перечням издаваемых конфиденциальных документов.

Издаваемые на предприятии конфиденциальные распорядительные документы (постановления, приказы, распоряжения), а также протоколы, помимо учетного номера, должны иметь ежегодную порядковую нумерацию в пределах каждого из этих видов документов. Для обеспечения последовательности проставления таких номеров, ускорения поиска документов могут вестись журналы (карточки) учета изданных конфиденциальных распорядительных документов и протоколов по каждому их виду отдельно. Журнал (карточка) имеет следующую форму.

Журнал (карточка) учета _____

(вид документов)

Порядковый №	Дата	Учетный № и гриф конфиденциальности	Заголовок	Кол-во экземпляров	Кол-во листов в экземпляре	Местонахождение
1	2	3	4	5	6	7

При карточном учете под каждый вид документов заводится своя карточка. При журнальном учете допускается некоторые виды документов вести совместно, но отдельными разделами (на разных страницах), за своими номерами.

В графе 3 проставляется учетный номер документа, присвоенный ему по журналу учета изданных документов. Графы 1 — 4 и 7 являются обязательными.

Глава VII

ПОЛУЧЕНИЕ (ОТПРАВЛЕНИЕ) КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ И ИХ УЧЕТ

Последовательность работы с поступившими (входящими) конфиденциальными документами показана на схеме 3.

Конфиденциальные документы пересылаются (доставляются) между организациями (предприятиями) в соответствующем образом оформленных и запечатанных конвертах (пакетах) и принимаются сотрудниками конфиденциального делопроизводства.

Если в организации (на предприятии) вся входящая корреспонденция поступает в экспедицию (или открытое делопроизводство), а также при получении пакетов в нерабочее время дежурным (сотрудником охраны), пакеты с конфиденциальными документами не вскрываются, а передаются в подразделение конфиденциального делопроизводства в нераспечатанном виде (под роспись). В этом случае полученные пакеты предварительно учитывают (принимают) по журналу экспедиции (открытого делопроизводства) или делают соответствующую запись о приеме пакета в книге дежурств.

Все документы (пакеты с документами), поступающие из других организаций (от предприятий), подлежат учету в подразделении конфиденциального делопроизводства по журналу, имеющему форму, представленную на с. 63.

Журнал поступивших документов ведется в течение календарного года.

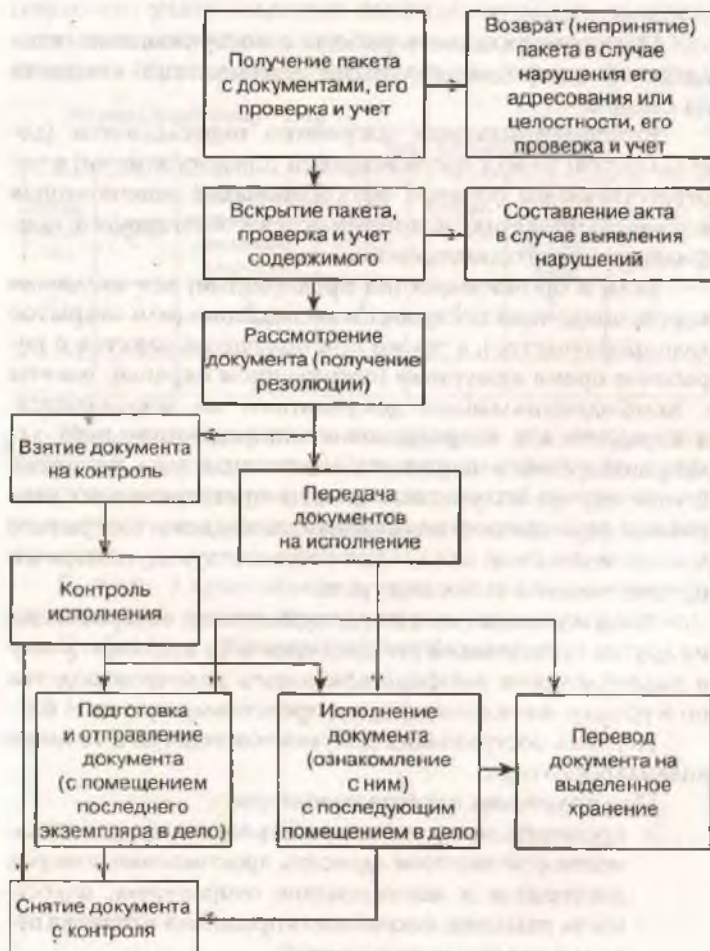
При получении пакетов необходимо:

- проверить на пакете наличие грифа конфиденциальности, соответствие адресата, проставление номеров документов и наименование отправителя, целостность упаковки, сохранность прошивки и оттиска печати (если они применяются);

- проверить в сопроводительном документе на пакете (реестре и др.) соответствие наименований адреса и отправителя, номеров документов, номеров экземпляров (если есть), грифа конфиденциальности;
- расписаться в сопроводительном документе за принятые пакеты с проставлением даты (при необходимости и времени) и печати (штампа).

Схема 3

Последовательность работы с поступившими (входящими) конфиденциальными документами



Журнал учета поступивших документов

Дата поступления пакета (документа)	№ реестра или подпись славшего пакет (документ)	Откуда поступил	№ и гриф поступившего документа, дата издания	Входящий № документа (№ экз.) и гриф конфиденциальности	Вид и заголовок документа	Кол-во листов документа	Кол-во листов приложени
1	2	3	4	5	6	7	8

Продолжение

Кому выдан	Кол-во листов	Подпись за получение и дата	Подпись за возврат и дата	Место хранения (№ дела, №№ листов)	№ по учету выделенного хранения, кол-во листов	Примечание (отметка о возврате документа)
9	10	11	12	13	14	15

Если на пакетах указан другой адресат, то они не принимаются.

При нарушении оформления пакетов, несоответствии данных на пакете и в сопроводительном документе, повреждении упаковки составляется акт в двух экземплярах, который подписывается сотрудниками, принимающими пакеты. Если обнаружены внешние повреждения пакета, то в акт целесообразно включить и подпись лица, доставившего этот пакет (при возможности). Второй экземпляр акта направляется отделению связи или отправителю пакета (если пакет доставлен, минуя отделение связи). Если повреждение пакета дает возможность изъять документ или прочесть его, то об этом сообщается руководителям получающей и отправляющей организаций (предприятий).

При вскрытии пакетов проверяется соответствие на пакете и документе наименования отправителя и адресата, грифа конфиденциальности, номеров документов, номеров экземпляров документа (если указаны на пакете). Пакеты должны быть развернуты таким образом, чтобы убедиться, что в них не осталось вложений. В документах проверяется наличие листов, а в документах, имеющих приложения, кроме того, соответствие учетных номеров, грифа конфиденциальности, номеров экземпляров, количества листов приложения записям в отметке о наличии приложения, содержащимся в основном документе (сопроводительном письме).

Пакеты с пометкой «Лично» вскрываются лицом, которому они адресованы, или уполномоченным им лицом. По усмотрению лица, вскрывшего пакеты, вышеперечисленные данные проверяются им самим или сотрудником подразделения конфиденциального делопроизводства. По пакетам, имеющим пометку «Лично», в журнале учета первоначально заполняются только графы 1 — 3.

При несоответствии на пакете и документе или на документе и приложении учетных номеров, несовпадении грифов конфиденциальности, недостатке (излишке) листов и экземпляров, а также в случае, если документ направлен ошибочно, подразделением конфиденциального делопроизводства (с участием лица, вскрывшего пакет) составляется акт в двух экземплярах, второй экземпляр вместе с лицевой стороной пакета (при несоответствии данных на пакете и документе) направляется отправителю.

Ошибочно присланные документы, лишние листы и экземпляры вместе с актом в новом пакете с сопроводительным письмом направляются отправителю. В графе 15 журнала учета поступивших документов производится отметка о возврате с указанием количества листов или номеров экземпляров, подлежащих возврату, и причины возврата, номера и даты сопроводительного письма, например: «Три листа (или экз. № ____) возвращены как лишние с № 25-КТ от 05.06.2006» или при возврате документа полностью: «Документ возвращен как ошибочно присланный с № 50-ДСП от 05.06.2006». Ошибочно присланные документы могут по согласованию с отправителем пересылаться по назначению, за его учетными номерами в новых пакетах с вложением в них лицевой стороны пакета отправителя. В этом случае в графе 15 журнала учета поступивших документов делается отметка о пересылке с указанием организации (предприятия), которой направлен документ, номера и даты сопроводительного письма.

Номера, грифы конфиденциальности (аббревиатурой), присвоенные документу отправителем, и даты документов проставляются в графе 4. Если указаны номера экземпляров, то они также переносятся в эту графу.

Порядковые (входящие) номера поступивших документов проставляются последовательно в течение года в графе 5, гриф конфиденциальности проставляется аббревиатурой. Для того чтобы отличить учетный номер поступивших (входящих) документов, используется шифр, который ставится перед номером, например «Вх. № 50-ДСП», или добавляется непосредственно к номеру, например «№ П 25-КТ».

В момент регистрации заполняются графы 1 — 8. Если документ прислан без сопроводительного письма, то в графе 7 проставляется количество его листов, а в графе 8 делается прочерк. Если документ имеет сопроводительное письмо, то в графе 7 проставляется количество листов сопроводительного письма, а в графе 8 количество листов приложений. При этом если все приложения имеют гриф конфиденциальности, указывается общее количество листов всех приложений, если часть приложений не имеет грифа конфиденциальности, то количество их листов проставляется через знак «+» к листам конфиденциальных приложений, например: «8 + 4 л/к». При поступлении документа в двух и более экземплярах проставляется общее количество листов всех экземпляров.

На самом документе в правом углу нижнего поля первого листа проставляется отметка о поступлении, которая содержит входящий номер, присвоенный документу, гриф конфиденциальности, дату поступления, количество листов. При наличии сопроводительного письма указывается отдельно количество листов письма и через знак «+» общее количество листов всех конфиденциальных приложений. При наличии открытых приложений количество их листов отражается отдельно через знак «+» с добавлением «н/к» (не конфиденциальные), например:

Вх. № 25-КТ 05.06.2006. л. 1 + 20 + 6 н/к

Если отметка проставляется с помощью штампа, то он может иметь следующую форму.

Вх. №	
Дата	
Кол-во лист.	

При наличии приложений, кроме отметки о поступлении документа, на первом листе каждого приложения (как конфиденциального, так и открытого) в правом углу нижнего поля проставляется штампом или пишется «К вх. № _____» с указанием номера, присвоенного документу в целом, и аббревиатурой его грифа конфиденциальности. Эта отметка необходима для того, чтобы в случаях получения исполнителем отдельных приложений без сопроводительного письма было видно, что они являются частью поступившего документа, а не отдельно изданным документом.

В сброшюрованных документах отметки о поступлении можно проставлять на титульном листе.

Присланные машинные носители регистрируются в журнале учета поступивших документов, а затем в журнале учета машинных носителей.

Если поступивший документ подлежит выделенному хранению, то ему следует сразу (без присвоения входящего учетного номера) присваивать очередной порядковый номер по журналу учета документов выделенного хранения (см. гл. VIII). Этот номер проставляется на докумен-

те, в журнале учета документов выделенного хранения и переносится в графу 14 журнала учета поступивших документов.

Если в организацию (на предприятие) возвращены без сопроводительного письма отправленные ранее без сопроводительного письма все или часть экземпляров документа, зарегистрированного по любому виду учета, или машинный носитель, то в журнале учета поступивших документов в графе 4 проставляется номер, ранее присвоенный документу.

Одновременно в журнале учета изданных документов или в журнале учета документов выделенного хранения (см. гл. VIII) делается отметка о возврате документа с проставлением даты возвращения и номера реестра. Такая отметка делается для возвращенных исходящих (изданных) документов текущего года (для документов выделенного хранения — текущего учета). Допускается возвращенному документу присваивать новый учетный номер.

Если документ (носитель) отправлялся и/или возвращен с сопроводительным письмом, то это письмо регистрируется за очередным номером в журнале учета поступивших документов, а документ, подлежащий выделенному хранению, переводится затем без сопроводительного письма на учет документов выделенного хранения (носитель — на учет машинных носителей). Сопроводительное письмо подшивается в дело. Допустимо также в журнале учета поступивших документов регистрировать только сопроводительное письмо, а приложение оформлять как возврат ранее отправленного документа. В обоих случаях на сопроводительном письме следует делать отметку об учетном номере и местонахождении приложения.

Поступившие документы должны обрабатываться и передаваться на рассмотрение соответствующему должностному лицу в день их получения или не позднее следующего рабочего дня и оперативно доводиться до исполнителей.

Отправление конфиденциальных документов в другие организации (на предприятия) производится аналогичным порядком, или в обратной последовательности. Конверты (пакеты), в которых отправляются документы, должны быть светонепроницаемыми или иметь вкладки из светонепроницаемой бумаги. Если одному адресату на-

правляются несколько документов, то они по возможности помещаются в один пакет. В правом верхнем углу пакета проставляется гриф конфиденциальности. На пакете пишется адрес и наименование получателя, а при наличии пометки «Лично» дополнительно должность, инициалы и фамилия адресата. Под адресатом перечисляются учетные номера документов, которые будут вложены в пакет (если документ отправляется с сопроводительным письмом, то на пакете проставляется только номер сопроводительного письма без указания номеров приложений). При направлении документов в двух и более экземплярах на пакете рядом с номером документа в скобках указываются номера экземпляров. Ниже проставляются адрес и наименование отправителя. При необходимости на пакете в центре верхнего поля может проставляться штамп «Срочно».

Перед помещением конфиденциальных документов в подготовленные пакеты проверяется соответствие данных на документах и пакетах, просчитывается количество листов и соответствие их учетным данным. При наличии сопроводительного письма проверяется, кроме того, соответствие названия, учетного номера, грифа конфиденциальности, номера экземпляра, количества листов приложения (с просчетом листов с записями в сопроводительном письме). Со стороны клапана в пакет может помещаться прокладочный лист (вставка).

Для обеспечения надлежащей сохранности документов пакет, в котором они пересылаются, рекомендуется заклеивать силикатным клеем и прошивать крест-накрест через середину нитками с захватом всех клапанов либо, если вложения нельзя прокалывать, через четыре края с тугим охватом краев вложений. Нитки завязываются в центре оборотной стороны пакета, на узел прошивки накладывается бумажная наклейка из папиросной или другой тонкой, но не расслаивающейся бумаги с оттиском печати подразделения конфиденциального делопроизводства. Наклейка должна быть на 2—4 мм больше размера оттиска печати. Наклейка накладывается так, чтобы захватывала все клапаны пакета в середине, концы ниток не находились под наклейкой, а узел прошивки был ею накрыт. Наклейка сверху покрывается тонким слоем силикатного клея, чтобы образовалась стекловидная прозрачная пленка. Размер пленки должен быть на 2—4 мм больше наклейки.

Пакеты с конфиденциальными документами могут доставляться через спецсвязь, почтовое отделение или курьером (непосредственно адресату). Возможно отправление пакетов и фельдъегерской связью. Пересылка пакетов фельдъегерской и специальной связью осуществляется на договорной основе. Через почтовое отделение связи пакеты пересылаются ценными или заказными отправлениями в соответствии с почтовыми правилами.

При отправлении пакетов с конфиденциальными документами через почтовое отделение связи в целях сокрытия конфиденциальности их целесообразно помещать в другие конверты, на которые наносятся только реквизиты, предусмотренные почтовыми правилами для открытых ценных и заказных отправлений. В этом случае пакеты поступают в подразделение открытого делопроизводства получателя и после вскрытия наружного конверта передаются (под расписку) в подразделение конфиденциального делопроизводства.

При пересылке корреспонденции фельдъегерской или специальной связью в необходимом количестве экземпляров составляется реестр, последний экземпляр которого остается у отправителя. Передача пакетов осуществляется в соответствии с правилами этих служб связи.

Доставка пакетов с конфиденциальными документами адресатам может осуществляться, с разрешения руководителя организации (предприятия), сотрудником подразделения конфиденциального делопроизводства либо другим работником, допущенным к конфиденциальной информации (курьером), на служебном транспорте. Пакеты передаются по реестру, в котором, кроме подписи о получении пакетов, должна быть проставлена печать получателя. Реестры грифа конфиденциальности не имеют.

Об отправленных документах производятся соответствующие отметки в учетных формах: в журнале учета изданных документов, в журнале учета документов выделенного хранения. При этом если документ отправлен без сопроводительного письма, то в графе «Наименование, номер и дата сопроводительного документа» пишется «реестр», «расписка», «квитанция», «накладная», если с сопроводительным письмом — «сопроводительное письмо» с проставлением номеров и дат этих документов.

Если по каким-либо причинам отправлен документ (или часть его), зарегистрированный в журнале учета поступивших документов, то отметка об отправлении представляется в этом журнале. В ней указываются количество отправленных листов, куда они направлены, наименование, номер и дата сопроводительного документа.

При необходимости, допускается вести отдельный учет отправляемых документов. В этом случае к исходящему номеру, как правило, добавляется определенный буквенный или цифровой идентификационный шифр, например: «150/___» (см. Приложение 6).

Документы, подлежащие отправке, должны обрабатываться и отправляться в день их подписания или не позднее следующего рабочего дня.

Глава VIII

УЧЕТ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ ВЫДЕЛЕННОГО ХРАНЕНИЯ

Учет документов выделенного хранения охватывает все документы, не подлежащие подшивке в дела. Такие документы можно разделить на две категории.

К первой относятся документы, которые по производственным условиям нецелесообразно подшивать в дела, например, различного рода инструкции, справочники, с которыми могут параллельно работать несколько исполнителей. При их подшивке исполнитель, взявший дело, лишает остальных исполнителей возможности пользоваться необходимыми им документами.

Ко второй категории относятся документы, которые по их внешним особенностям невозможно или нецелесообразно подшивать в дела (большого формата, сброшюрованные, чертежно-графические и т. д.).

На учет выделенного хранения могут также ставиться рабочие тетради исполнителей (пользователей).

Для того чтобы отличить учетный номер документов выделенного хранения, используется шифр, который ставится перед номером, например «Ив. № 50-ДСП» (инвентаризационный номер), или добавляется непосредственно к номеру, например «№ В 25-КТ».

Учет конфиденциальных документов, подлежащих выделенному хранению, осуществляется в журналах (карточках) учета, имеющих форму, представленную на с. 72.

При значительном объеме документов выделенного хранения чертежно-графические и текстовые документы могут учитываться раздельно, но в однотипных формах учета. В этом случае слова «чертежно-графические» или «текстовые» должны включаться в наименование журнала.

На учет выделенного хранения документы могут ставиться непосредственно при их поступлении или создании,

Журнал учета конфиденциальных документов выделенного хранения

Учетный (инв.) № и триф коэффи- циентально- сти	Дата реги- страции	Вид и заго- ловок доку- мента	Откуда по- ступил (кем разработан)	С какого учетного но- мера	№№ экземп- ляров	Кол-во листов в экземпляре
1	2	3	4	5	6	7
Продолжение						
Место- нахождение	Отметка о картотеке	Отметка об отправке	Отметка о возврате	Отметка о сня- тии с учета вы- деленного хра- нения	Отметка об уничтожении	
8	9	10	11	12	13	

а также переводиться с других видов учета (по мере необходимости). Снятие документов с учета выделенного хранения может быть при их подшивке в дела, отправке или уничтожении. При отправке документа с последующим возвратом (во временное пользование) снятие с учета не производится.

В момент регистрации документа по журналу учета заполняются графы 1 — 7.

При регистрации чертежно-графических документов в графе 3 проставляются вид носителя (калька, ватман) и индекс (обозначение) документа.

При взятии на учет документа, переводимого с учета поступивших документов, в графе 4 указывается, откуда поступил документ, в графе 5 — его учетный номер по журналу учета поступивших документов. Одновременно в графе 14 журнала учета поступивших документов проставляются номер, присвоенный документу по журналу учета документов выделенного хранения, и количество листов, переведенных на выделенное хранение.

Местонахождение документа (графа 9) указывается для каждого экземпляра документа (графы 6, 7).

При взятии на учет документа, переводимого с учета изданных документов, в графе 4 указывается подразделение, разработавшее документ, в графе 5 — учетный номер документа по журналу учета изданных документов. В графе 16 журнала учета изданных документов проставляются номер, присвоенный документу по журналу учета документов выделенного хранения, и количество переведенных на выделенное хранение экземпляров.

Взятые на учет выделенного хранения текстовые документы помещаются в обложку и брошпуруются (прошиваются), если ранее не имели обложки и не были сброшпурованы. При этом после последнего листа документа помещается лист с заверительной надписью (штампом), в которой указывается прописью количество листов в документе, заверяемое подписью сотрудника конфиденциального делопроизводства, с проставлением даты. Если в документе имеются литературные, пропущенные номера или вклеенные на листы фотографии, то они оговариваются в заверительной надписи.

На текстовых документах учетные номера, присвоенные по журналу учета документов выделенного хранения, проставляются в верхнем левом углу обложки и титульного ли-

ста (при его наличии). В правом верхнем углу проставляются гриф конфиденциальности и под ним номер экземпляра.

На чертежно-графических документах учетные номера проставляются на каждом листе в местах, отведенных соответствующими стандартами. На присланных документах имеющиеся там номера зачеркиваются (гонкими линиями).

На каждый документ (экземпляр документа) заводится отдельная карточка учета временной выдачи документа. Карточка хранится в документе (желательно во вклеенном открытом конверте), а при его выдаче помещается в специально выделенное место для хранения и контроля.

Карточка имеет следующую форму.

Карточка учета выдачи конфиденциального документа (дела)

Учетный №, гриф конфиденциальности, наименование документа, количество листов)

Кому выдан документ	Кол-во листов	Подпись за получение и дата	Подпись за возврат и дата
1	2	3	4

С выданным документом пользователь может работать в помещении конфиденциального делопроизводства или на своем рабочем месте, если оно соответствующим образом оборудовано. Выданный документ подлежит сдаче в подразделение конфиденциального делопроизводства в этот же день или (если это разрешено) может оставаться у исполнителя.

Требования к оборудованию помещений, в которых разрешено работать с конфиденциальными документами, изложены в гл. XIII. Порядок работы исполнителей с конфиденциальными документами устанавливается в одном из разделов «Положения о режиме коммерческой (служебной) тайны организации (предприятия)».

Журнал учета документов выделенного хранения ведется непрерывно. Номера каждого года продолжают номера предыдущих лет. Вызвано это тем, что выделенному хранению подлежат, как правило, документы долговременного хранения, и их ежегодная перерегистрация нецелесообразна. Такая перерегистрация осуществляется по мере необходимости.

Для ведения тематического учета документов целесообразно создавать отдельные картотеки (по форме библиотечных картотек), позволяющие осуществлять быстрый поиск необходимых изданий. В графе 10 журнала учета документов выделенного хранения делается отметка, в какой картотеке (если их несколько) помещена тематическая карточка с реквизитами этого документа.

В тематической карточке указывают учетные номера документа, гриф конфиденциальности, количество листов, его местонахождение, фамилию и инициалы автора (или наименование организации издавшей документ), краткое содержание документа, год издания и другие необходимые для данной картотеки отметки. Карточки помещаются в специальные ячейки в алфавитном порядке. Желательно предусмотреть фиксацию карточек в этих ячейках (стержнем или нитью, проходящими через перфорацию карточек) для удобства и сохранности.

Карточкам учета выдачи документа и тематическим карточкам гриф конфиденциальности не присваивается. Их уничтожение производится вместе с документами, для которых они заведены.

Глава IX

УЧЕТ КОПИРОВАНИЯ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

При действительной служебной необходимости в дополнительных экземплярах копифиденциальных документов производится их копирование.

Следует иметь в виду, что на некоторых конфиденциальных документах может стоять отметка о том, что снятие копий с этого документа не разрешается. В этом случае документ может также иметь дополнительную защиту от ксерокопирования или сканирования (с уничтожением текста при попытке снять копию). Такие документы копированию не подлежат.

Конфиденциальные документы могут копироваться в подразделении конфиденциального делопроизводства или в специальном множительном подразделении организации (предприятия).

Предназначенные для копирования документов технические средства (копировально-множительное оборудование, компьютеры, пишущие машинки) должны быть защищены от возможного перехвата возникающих при их работе электромагнитных излучений.

Копирование конфиденциальных документов не должно производиться одновременно с копированием открытых документов. Во время копирования доступ посторонних лиц в помещение, в котором производятся работы, не допускается.

Разрешение на копирование (снятие копий) документов могут давать соответствующие должностные лица (руководители подразделений), наделенные правом распоряжения конфиденциальными сведениями. Список лиц, имеющих право давать разрешение на копирование конфиденциальных документов, должен быть закреплен в одном из разделов «Положения о режиме коммерческой (служебной) тайны организации (предприятия)».

Конфиденциальные документы, поступившие из других организаций (предприятий), должны копироваться с письменного разрешения руководителя организации (предприятия) или с письменного разрешения издавших их организаций (предприятий).

Копирование документов производится методами изготовления дополнительных экземпляров (тиражирования), снятия копий с документов и производства выписок из документов.

Дополнительно отпечатанные экземпляры подлежат учету, а в необходимых случаях — заверению как копии.

Разрешение на изготовление дополнительных экземпляров (копий) учетного документа оформляется на обороте последнего листа экземпляра, с которого производится копирование. Этот экземпляр не должен в последующем направляться в другие организации (на предприятия), он подшивается в дело или переводится на учет документов выделенного хранения.

Разрешение оформляется, как правило, специальным штампом, где проставляются номера документов или страниц, с которых необходимо сделать копию.

При копировании поступившего документа дополнительно делается ссылка на номер и дату разрешения.

Штамп разрешения имеет следующую форму.

Копирование _____ <i>(№ документа, номера страниц)</i>
в _____ экз. разрешаю. <i>(прописью)</i>
_____ <i>(должность, подпись)</i>
« » _____ 20 г.

При невозможности оформления разрешения на копирование на самом документе оно оформляется в графах учетной формы данного документа. При копировании документов в множительном подразделении их передача на копирование производится должностному лицу этого подразделения под его роспись в учетной форме или карточке выдачи документа.

Подлежащие копированию документы регистрируются в подразделении конфиденциального делопроизводства

или в множительном подразделении (по месту копирования) в журнале учета копирования конфиденциальных документов, имеющего следующую форму.

Журнал учета копирования конфиденциальных документов

Учетный №, гриф конфиденциальности и дата документа	Кол-во или №№ страниц	Дата копирования	Кол-во снятых копий (листов или экземпляров)	Учетные №№, присвоенные копиям (экземплярам)	Отметка об уничтожении брака (кол-во листов, подпись)	Подпись за получение и дата
1	2	3	4	5	6	7

При поступлении документа на копирование заполняются графы 1 – 2 журнала. В графе 1 гриф конфиденциальности проставляется аббревиатурой. В графе 2 указывается общее количество копируемых страниц документа.

Если копируется документ своей организации (предприятия), то в процессе копирования номер экземпляра документа, с которого осуществляется копирование, на копиях не воспроизводится. При копировании поступивших документов номер экземпляра воспроизводится.

Учетный номер, присвоенный документу, сохраняется на всех копиях.

После копирования документа заполняются графы 3, 4 и (при наличии брака) 6 журнала учета копирования конфиденциальных документов. В графе 4 указывается общее количество копий экземпляров (или листов) без проставления их номеров. В графе 6 отражается общее количество листов брака без перечисления их номеров. Эти листы уничтожаются установленным порядком, с проставлением подписей двух сотрудников конфиденциального делопроизводства (множительного подразделения).

Графа 7 включается в журнал и заполняется в случаях, когда копирование производится в множительном подразделении. Подпись за возврат документа, с которого производилось копирование, проставляется в учетной форме, по которой осуществлялась его передача в множительное подразделение.

На копиях экземпляров документа сотрудник конфиденциального делопроизводства проставляет их номера. При этом если документ был издан самой организацией (предприятием), то номера копий продолжают номера ранее изготовленных экземпляров. Если документ был издан другой организацией (предприятием), то на копиях их номера проставляются дробно: в числителе на всех экземплярах остается номер, присвоенный при издании документа, а в знаменателе на каждом экземпляре проставляется очередной порядковый номер копии, начиная с № 1.

На каждой копии в реквизите «Отметка об исполнителе» проставляется только учетный номер, присвоенный документу при его издании, независимо от места издания.

На экземпляре, с которого производилось копирование, под разрешением на копирование сотрудник конфиденциального делопроизводства производит запись: «Размножено _____ экз.», которая заверяется его подписью с проставлением даты. Указанная надпись может проставляться штампом.

Если на копиях документов подпись не воспроизводится, то они удостоверяются печатью подразделения конфиденциального делопроизводства, которая проставляется с захватом части слова, обозначающего должность лица, подписавшего документ.

При копировании документов, зарегистрированных в журнале учета изданных документов, количество копий экземпляров проставляется в графе 6 этого журнала, ниже ранее проставленных через знак «+».

При копировании документов, зарегистрированных по журналу учета поступивших документов, отметка о копировании производится в графах 6, 7 этого журнала ниже ранее проставленных листов и оформляется следующим образом: «Размножено _____ экз.».

При копировании документов, зарегистрированных в журнале учета документов выделенного хранения, отметка о копировании производится в графах 6, 7 этого журнала. Номера копий экземпляров проставляются следом за ранее проставленными номерами через знак «+».

Технология копирования конфиденциальных документов, подшитых в дело и, соответственно, снятых с учета по журналам (карточкам) учета этих документов, аналогична

технологии изготовления дополнительных экземпляров. Но в этом случае копии документа присваивается отдельный учетный номер — очередной порядковый номер по журналу учета изданных документов, независимо от того, по какому виду учета (изданных или поступивших документов) зарегистрирован документ, с которого снимается копия.

Присвоенный копии учетный номер проставляется на всех листах копии посередине нижнего поля с добавлением аббревиатуры грифа конфиденциальности (на последнем листе — в реквизите «Отметка об исполнителе»). В реквизите «Дата и номер документа» на копии сохраняются прежние данные.

На первом листе копии над реквизитом «Гриф конфиденциальности документа» проставляется (желательно штампом) слово «КОПИЯ». Отметка «КОПИЯ» ставится всегда, когда на ней проставляются дополнительные номера экземпляров.

Реквизит «Отметка об исполнителе» оформляется полностью, как во вновь создаваемых документах.

Ниже реквизита «Подпись» на копии документа проставляется заверительный штамп или пишется слово «Верно», которое заверяется подписью лица, производившего снятие копии, с указанием его должности, инициалов и фамилии, а также даты. Если копия пересылается в другие организации (предприятия), то на ней дополнительно проставляется печать организации (предприятия) или подразделения конфиденциального делопроизводства.

Экземпляры копий имеют самостоятельную нумерацию, начиная с № 1 (Копия экз. № 1 и т. д.).

На экземпляре документа, с которого снималась копия, под разрешением на снятие копии сотрудником конфиденциального делопроизводства производится запись «Снята копия в _____ экз. за № _____», которая заверяется его подписью с проставлением даты.

В журнале учета копирования конфиденциальных документов дополнительно заполняется графа 5.

Заполнение граф журнала учета изданных документов при снятии копий производится аналогично заполнению на вновь создаваемые документы.

Что касается выписок, то они могут производиться как с не подшитых, так и подшитых в дела документов, а

также с документов выделенного хранения. Выпискам присваивается отдельный учетный номер — очередной порядковый номер по журналу учета изданных документов, независимо от того, по какому виду учета зарегистрирован документ, с которого производится выписка. Проставление учетного номера на выписке осуществляется аналогично проставлению его на копии.

На первом листе выписки после заголовка документа проставляется слово «ВЫПИСКА». Выписка имеет собственную нумерацию листов и экземпляров.

Реквизит «Отметка об исполнителе» оформляется полностью.

Отметки о производстве и заверении выписки оформляются так же, как и в копии, но с использованием слов «Произведена выписка».

В журнале учета копирования конфиденциальных документов в графе 2 перед производством выписки проставляются номера листов или пунктов, с которых производится выписка (например, л.л. 5 — 10 или п.п. 5, 10 — 15), а в графе 5 после производства выписки — учетный номер выписки, остальные графы заполняются как и при других формах копирования.

Заполнение граф журнала учета изданных документов при производстве выписок осуществляется аналогично их заполнению на вновь создаваемые документы.

ОРГАНИЗАЦИЯ ИСПОЛНЕНИЯ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

Организация исполнения конфиденциальных документов также имеет свои особенности.

При большом объеме поступающих документов целесообразно осуществлять их распределение по уровням принятия решений. С этой целью руководителем организации (предприятия) определяются полномочия подчиненных должностных лиц по рассмотрению (решению) вопросов определенной тематики или уровня, без предварительного ознакомления с этими документами непосредственно руководителя организации (предприятия). В необходимых случаях эти должностные лица докладывают такие документы вышестоящему руководителю самостоятельно.

Такое распределение поступивших конфиденциальных документов осуществляется непосредственно руководителем подразделения конфиденциального делопроизводства или помощником (референтом) руководителя организации (предприятия). Это лицо лишь адресует (передает на рассмотрение) документы руководителям различных уровней без указания порядка и сроков их исполнения. Характер и сроки исполнения документов определяются резолюциями этих руководителей.

Такой порядок позволяет сократить путь и время движения документов до непосредственных исполнителей, а следовательно, ускорить процесс их исполнения, освободить руководителей различного ранга от рассмотрения вопросов, которые могут быть решены на низших инстанциях, уменьшить трудозатраты на рассмотрение, исполнение и обработку документов.

Документы, передаваемые на рассмотрение руководителям, могут учитываться непосредственно в журнале учета поступивших документов (в графах 9–11) с после-

дующим занесением туда фамилий исполнителей, которым переадресован документ, или записываться в специально выделенный реестр временной передачи конфиденциальных документов. Запись документов в реестр на имя руководителя осуществляется в том случае, если они не рассматриваются в присутствии сотрудника конфиденциального делопроизводства, ответственного за их учет.

При одновременном получении и возврате нескольких документов может проставляться одна подпись за все документы (с указанием их количества).

Если после рассмотрения документов в присутствии сотрудника подразделения конфиденциального делопроизводства у руководителя остается часть их, то в реестр записывается только эта часть.

В процессе рассмотрения документов на них пишутся резолюции. В состав резолюции входят следующие элементы:

- инициалы и фамилия исполнителя (исполнителей);
- содержание поручения (предписываемое действие);
- срок исполнения (при необходимости);
- подпись;
- дата;
- отметка о контроле исполнения (при необходимости).

Текст (содержание) поручения должен быть конкретным и кратким.

Порядок оформления резолюций изложен в *Приложении б*.

Резолюция может оформляться на отдельном, прикрепляемом к документу листе (в том числе специальном листе с отпечатанным на нем названием должности лица, делающего резолюцию) с указанием учетного номера и даты документа, к которому относится резолюция.

В случаях, когда поручение дается двум и более лицам, ответственным исполнителем является лицо, указанное первым. Ему предоставляется право координации работы соисполнителей. Если ответственным исполнителем назначается лицо, указанное в резолюции не первым, то рядом с его фамилией в скобках или через тире проставляется «— отв.».

На документах, не требующих указаний по исполнению и срокам исполнения, резолюция не проставляется, а

должностное лицо ставит подпись за ознакомление с документом и дату такого ознакомления.

Резолюция пишется на поле между адресатом и текстом. Если она не помещается на этом поле, то ее можно писать на свободном месте первого листа (особенно если на документе проставляется резолюция следующего должностного лица или при внутреннем переадресовании документа по исполнителям), за исключением полей.

На документах, требующих дополнительного контроля исполнения, сверху проставляется реквизит «Отметка о контроле» (см. Приложение 6), который обозначается буквой «К» (как правило, красным цветом) либо словом или штампом «Контроль».

Целью отметки является указание подразделению конфиденциального производства о взятии документа на контроль по срокам исполнения.

После рассмотрения и написания резолюций на документах они передаются исполнителям под роспись в соответствующих учетных формах. Обязательность подписи за получение и возврат конфиденциальных документов независимо от занимаемой должности необходима для обеспечения сохранности документов и контроля сроков прохождения документов.

Если исполнителей несколько, то документ в первую очередь передается ответственному исполнителю, указанному в резолюции, а при отсутствии указания — лицу, поставленному в резолюции первым.

При получении документа исполнитель должен проверить соответствие учетного номера документа и количества его листов записям в учетных формах.

Передача документов между исполнителями, (только теми, кто указан в резолюции) должна производиться через подразделение конфиденциального делопроизводства или (при возврате в течение рабочего дня) по реестру (разовой расписке) — в этом случае минуя подразделение конфиденциального делопроизводства.

Ответственность за качество исполнения документов несут исполнители и руководители подразделений, в которых работают исполнители.

Если исполнение документа поставлено на контроль, то для его осуществления изготавливаются специальные контрольные карточки, имеющие следующую форму.

Карточка контроля исполнения документа

Срок исполнения _____

(учетный №, гриф конфиденциальности и дата документа)

Вид и заголовки документа	От кого поступил	Резолюция (должностное лицо и содержание)	Ответственный исполнитель	Контрольные отметки	Отметка о снятии с контроля
1	2	3	4	5	6

В контрольных карточках не должны содержаться конфиденциальные сведения.

При контроле документов, пункты которых имеют самостоятельного исполнителя и свой срок исполнения, на каждый из пунктов заполняется отдельный экземпляр контрольной карточки.

Из карточек контролируемых документов формируется контрольная картотека по срокам исполнения документов. В пределах каждого срока карточки могут систематизироваться по видам учета документов, исполнителям, видам документов и др.

При автоматизированном контроле исполнения документов соответствующие данные вводятся в компьютер.

В процессе контроля исполнения документа подразделение конфиденциального делопроизводства должно периодически (в установленные сроки) напоминать исполнителю о контролируемом документе, о чем в графе 5 карточки проставляется соответствующая дата. О нарушении срока исполнения документа подразделение конфиденциального делопроизводства докладывает руководителю, сделавшему резолюцию и поставившему документ на контроль.

Перечень должностных лиц, имеющих право ставить документы на контроль подразделения конфиденциального делопроизводства, указывается в соответствующем разделе «Положения о режиме коммерческой (служебной) тайны организации (предприятия)».

После исполнения документа исполнитель проставляет на нем отметку об исполнении документа и направлении его в дело.

Отметка содержит следующие данные:

- ссылку на дату и номер документа, свидетельствующего об исполнении данного документа, или при отсутствии такого документа краткую справку об исполнении;
- пометку «В дело»;
- номер дела, в которое должен быть подшит документ;
- подпись исполнителя или руководителя структурного подразделения, в котором исполнен документ;
- дату.

Например:

Исполнен 05.06.2006 № 25-КТ.

В дело № 50.

Подпись

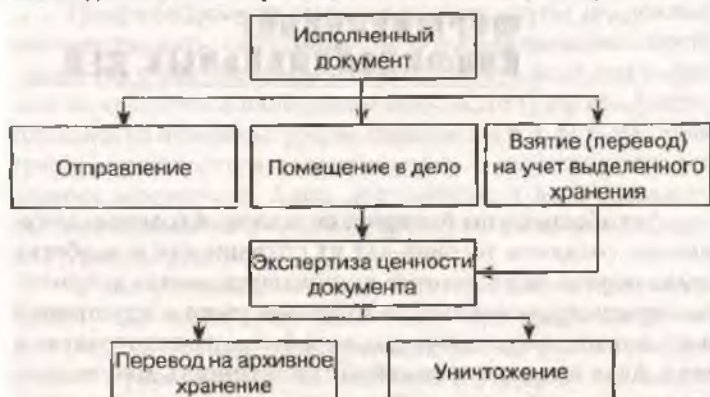
05.06.2006.

Исполненный документ вместе с документом-ответом (при наличии) сдается в подразделение конфиденциального делопроизводства. Сотрудник конфиденциального делопроизводства должен проверить правильность произведенной отметки об исполнении документа, соответствие вида и заголовка документа заголовку дела, в которое он направляется, просчитать количество листов документа и проверить соответствие их учетным данным, расписаться за получение документа в соответствующих графах учетных журналов. Контролируемый документ снимается с контроля, а контрольная карточка или уничтожается, или помещается в справочную картотеку.

Если конфиденциальный документ не требует исполнения, а адресован лишь для ознакомления, то он может не выдаваться на рабочее место исполнителя, а ознакомление с ним производится в подразделении конфиденциального делопроизводства. При этом если ознакомление производится в присутствии сотрудника конфиденциального делопроизводства, ответственного за учет документа, то подпись в учетной форме за получение документа может не проставляться. Подписи об ознакомлении с документами с проставлением даты производятся на самих документах, а подписи об ознакомлении с распорядительными документами могут проставляться на специальном листе ознакомления.

Схема 4

Последовательность работы с исполненными документами



После исполнения поступившего документа или ознакомления с ним соответствующих должностных лиц открытые приложения (без грифа), не подлежащие совместному хранению с основным конфиденциальным документом, передаются в подразделение открытого делопроизводства с заполнением журнала учета поступивших документов и с отметкой о передаче на основном документе (сопроводительным письмом).

Документы подлежат исполнению в следующие сроки:

- с конкретной датой исполнения — в указанный срок;
- с пометкой «Срочно» — в 3-дневный срок;
- по запросам граждан — в течение 15 дней;
- остальные — в срок не более месяца¹.

В общем виде дальнейшая последовательность работы с исполненными документами показана на схеме 4 и рассмотрена в соответствующих главах.

¹ Типовая инструкция по делопроизводству в федеральных органах исполнительной власти, утвержденная приказом Минкультуры России 2005 г. № 536.

Глава XI

ФОРМИРОВАНИЕ КОНФИДЕНЦИАЛЬНЫХ ДЕЛ

Для обеспечения быстрого поиска необходимых документов, создания условий для их сохранности и удобства пользования, исполненные конфиденциальные документы, зарегистрированные по журналам учета поступивших и изданных документов, должны быть сгруппированы в дела. Дело представляет собой совокупность документов (или отдельный документ), относящихся к одному вопросу или направлению деятельности и помещенных в отдельную обложку.

Распределение документов по делам производится в течение года по мере исполнения документов в соответствии с номенклатурой конфиденциальных дел.

Номенклатура конфиденциальных дел — это оформленный в установленном порядке систематизированный перечень наименований дел, заводимых в делопроизводстве, с указанием их условных номеров (индексов), сроков хранения и подразделений, которым предоставлено право пользования конкретными делами.

Номенклатура конфиденциальных дел является учетной формой для заведенных конфиденциальных дел и входит в систему доступа к конфиденциальным документам.

Номенклатура конфиденциальных дел должна, как правило, составляться отдельно от номенклатуры открытых дел.

Номенклатура конфиденциальных дел разрабатывается для организации (предприятия) в целом (сводная номенклатура дел). Она составляется на каждый год (в конце текущего года на следующий год) подразделением конфиденциального делопроизводства на основе предложений структурных подразделений.

Номенклатура подписывается руководителем подразделения конфиденциального делопроизводства, визируется руководителями заинтересованных структурных под-

разделений и утверждается руководителем организации (предприятия).

Гриф конфиденциальности номенклатуры дел должен соответствовать совокупной степени конфиденциальности сведений, содержащихся в заголовках дел. Если эти сведения не являются конфиденциальными, то гриф конфиденциальности номенклатуре не присваивается. При наличии грифа номенклатура регистрируется в журнале учета изданных документов. Лица, допущенные к делам, должны быть ознакомлены с соответствующими разделами номенклатуры под роспись.

После утверждения номенклатуры возможные в течение года изменения вносятся в нее подразделением конфиденциального делопроизводства на основании решений руководителя организации (предприятия) по докладным запискам руководителей подразделений.

Номенклатура конфиденциальных дел имеет форму, представленную на с. 90.

Предусматриваемые номенклатурой дела должны охватывать все управленческие конфиденциальные документы, которые предполагается издать или получить в течение года. В номенклатуру включаются также дело с номенклатурой дел, журналы (картотеки) всех видов учета конфиденциальных документов, дела с реестрами, квитанциями и расписками на конфиденциальные документы независимо от того, имеют или не имеют они гриф конфиденциальности.

Дела, ведущиеся в течение нескольких лет (переходящие дела), вносятся в номенклатуру каждого года с момента их заведения до закрытия.

Документы, зарегистрированные по журналу учета документов выделенного хранения, в номенклатуру не включаются.

Планируемая группировка документов (по делам) закрепляется в номенклатуре в заголовках дел. Заголовки должны в обобщенном виде отражать состав и содержание документов, подлежащих группировке в дело. Не допускаются заголовки типа «Общая (разная) переписка», «Руководящие материалы» и им подобные, которые не раскрывают содержания дел и нередко являются причиной неправомерного ознакомления пользователей с документами, находящимися в деле.

Наименование организации
(предприятия)

НОМЕНКЛАТУРА
КОНФИДЕНЦИАЛЬНЫХ ДЕЛ

на 20 ____ г.
№ _____

Гриф конфиденциальности
(при необходимости)

УТВЕРЖДАЮ

(должность, должность и фамилия)

(подпись, инициалы и фамилия)
« » _____ 20 ____ г.

№ дела и гриф конфиденциальности	Заголовки дела	Наименование подразделения, которому предоставляется дело	№ тома	Дата заведения тома (дела)	Дата закрытия тома (дела)	Кол-во листов в томе (дела)	Срок хранения и № статей по перечню	Архивный шифр, № и дата акта об уничтожении, отметки об отправке
1	2	3	4	5	6	7	8	9

Руководитель подразделения
конфиденциального делопроизводства

(подпись, инициалы и фамилия)
« » _____ 20 ____ г.

Согласующие визы должностных лиц
(руководителей структурных подразделений, архива, председателей экспертной комиссии)

Заголовок может включать в себя указание вида дела («документы», «переписка») или видов документов («договоры», «протоколы»), содержание документов (вопросов), время или место события.

Содержание документов указывается в заголовках всех дел, за исключением дел с распорядительными документами, которые подразделяются лишь по видам деятельности (например, приказы по финансовой деятельности, по кадрам), и протоколами, которые подразделяются по принадлежности (например, протоколы совещаний научно-технического совета).

Использование в заголовках других уточняющих слов, допускается в тех случаях, когда они несут в себе необходимую информацию и без их наличия теряются индивидуальные особенности заголовка или возникает его двоякое понимание. В заголовках дел с планово-отчетной документацией указывается периодичность документации, например: «Месячные планы...».

При составлении заголовков дел необходимо предусматривать:

- группировку документов в дело, как правило, по одному вопросу (за исключением распорядительных документов и протоколов);
- группировку распорядительных документов по видам документов (приказы, распоряжения, постановления, решения);
- раздельную группировку документов постоянного и временного сроков хранения;
- группировку документов с учетом распределения обязанностей между исполнителями;
- группировку приложений к документам вместе с документами, к которым они относятся (исключение допускается для больших по объему приложений, для которых могут предусматриваться отдельные дела);
- группировку документов по планированию текущего года, отдельно от документов по планированию следующего года.

Все это позволяет в значительной мере предотвращать ознакомление исполнителей с документами, не имеющими к ним отношения по роду выполняемой работы.

Дела с планами и отчетами располагаются в последовательности сроков их хранения: вслед за делами с годовыми планами (отчетами) должны вноситься дела с квартальными, а затем с месячными планами (отчетами). Дела с перепиской по одному вопросу, различающиеся между собой корреспондентским признаком, располагаются по алфавиту корреспондентов, а дела с документами, различающиеся географическим признаком, — по названиям населенных пунктов (в алфавитном порядке).

При значительном количестве дел целесообразно группировать их в номенклатуре по разделам, соответствующим наименованиям структурных подразделений или основным направлениям (вопросам) деятельности предприятия. Каждому разделу присваивается номер, например: 05 — Плановый отдел (при структурной схеме), 10 — Финансирование (при производственно-отраслевой схеме).

Дело с номенклатурой конфиденциальных дел, конфиденциальные и открытые журналы (картотеки) учета конфиденциальных документов, а также открытые дела с материалами на конфиденциальные документы (реестры, квитанциями на отправленные документы, актами проверок наличия документов и др.) помещаются в конце номенклатуры, не имеющей деления по разделам, а при наличии разделов — в разделе, соответствующем названию подразделения конфиденциального делопроизводства (при структурной схеме построения номенклатуры дел), или в разделе «Конфиденциальное делопроизводство» (при производственно-отраслевой схеме построения).

Каждому делу присваивается самостоятельный цифровой индекс, который состоит из номера структурного подразделения (при структурной схеме построения номенклатуры) или номера направления (при производственно-отраслевой схеме) и порядкового номера дела в пределах каждого раздела, например: «Дело № 0101» или «Дело № 1001» и т. д. В номенклатуре, не имеющей деления на разделы, вместо индекса дела проставляется его порядковый номер по номенклатуре, например: «Дело № 20».

При делении номенклатуры на разделы перед группой дел раздела проставляются номер и название раздела. Разделы следует начинать с нового листа или оставлять между ними свободное место для возможной регистрации в течение года новых дел.

В графе 1 указываются индекс или номер дела (учетного журнала) и его гриф конфиденциальности. Переходящим делам индексы (номера) сохраняются на весь период ведения дела.

В графу 2 вносится заголовок дела. Переходящим делам заголовки сохраняются до их закрытия. При закрытии дела заголовок может корректироваться, все изменения переносятся в номенклатуру.

В графе 3 перечисляются подразделения, которым предоставляется право пользования соответствующим делом.

Графы 1–3 заполняются при составлении номенклатуры.

В графах 4, 5 проставляются арабскими цифрами номер каждого тома и дата его заведения. Графы заполняются в день подшивки первого документа тома дела (заполнения первой позиции учетного журнала, составления первой учетной карточки). Если дело переходящее, то в графе 5 при составлении номенклатуры указывается: «Переходящее с 20__ г.», с проставлением года заведения дела.

В графе 6 проставляется арабскими цифрами дата закрытия каждого тома. Графа заполняется в день закрытия тома. Если дело переходит на следующий год, то в графе указывается: «Переходит на 20__ г.».

В графе 7 проставляется количество листов в томе (без учета листов описи документов дела). Графа заполняется при заведении учетного журнала и при закрытии тома дела, картотеки.

Графы 4–7 заполняются по каждому тому отдельной строкой.

В графе 8 проставляются срок хранения и номера статей (их может быть несколько) по установленному перечню документов с указанием сроков хранения (*подробнее о перечнях см. следующую главу*). При отсутствии соответствующих статей в перечнях сроки хранения дел устанавливаются экспертной комиссией. Графа заполняется при составлении номенклатуры дел. При закрытии дела и проведении экспертизы ценности документов дела срок хранения и номера статей могут корректироваться, изменения должны быть перенесены в номенклатуру дел.

В графе 9 проставляются архивный шифр дела, если дело передано в архив (№ фонда, описи, единицы хране-

ния), или номер и дата акта об уничтожении дела, или, если дело направлено в другую организацию (на предприятие), наименование адресата, номер и дата сопроводительного документа (письма, реестра, квитанции). Графа заполняется после проведения соответствующих операций.

При заведении дел, не предусмотренных номенклатурой, они вносятся в соответствующий раздел номенклатуры в день заведения (принятия решения о внесении изменений в номенклатуру). Дела, поступившие из других организаций (предприятий), вносятся в соответствующие разделы номенклатуры с проставлением дат их фактического заведения и закрытия.

Если предусмотренное номенклатурой дело не было заведено, то по окончании года в графе 9 проставляется отметка: «Дело не заводилось».

На каждое дело (том дела) при его заведении оформляется карточка учета временной выдачи дела. Карточка имеет такую же форму, как и карточка выдачи документов выделенного хранения (см. гл. VIII). Карточка помещается в открытый конверт, прикрепленный к внутренней стороне обложки дела.

Непосредственное формирование дел включает распределение документов по делам в соответствии с номенклатурой и систематизацию документов внутри дел. Дела формируются в течение года по мере поступления в них документов.

Формирование конфиденциальных дел должно осуществляться в подразделении конфиденциального делопроизводства.

В дела помещаются исполненные документы (подлинники, заверенные экземпляры), оформленные в установленном порядке. Другие экземпляры могут помещаться в дело лишь в случаях, когда на них имеются какие-либо резолюции или записи, дополняющие содержание основного экземпляра. При производственной необходимости допускается помещать в дела проекты документов. В исключительных случаях с разрешения руководителя подразделения конфиденциального делопроизводства допускается помещать в конфиденциальные дела отдельные открытые документы, имеющие прямое отношение к содержанию конфиденциальных документов дела.

В дела не должны помещаться документы, подлежащие возврату (отправке).

Перед помещением документа в дело сотрудник подразделения конфиденциального делопроизводства обязан проверить наличие отметки об исполнении, соответствие вида и содержания документа заголовку дела, наличие отметки о переводе приложения на учет конфиденциальных документов выделенного хранения (если оно не подшивается в дело).

В деле группируются, как правило, документы одного календарного года. При необходимости, по отдельным вопросам допускается ведение переходящих дел. В зависимости от вида и содержания документы систематизируются внутри дел в вопросно-логической, хронологической последовательности или их сочетании.

Изданные распорядительные документы, протоколы, акты систематизируются в делах в порядке возрастания номеров.

В делах с перепиской поступившие документы помещаются вместе с копиями отправленных документов, которыми они исполнены. Копии изданных инициативных документов, направляемых в другие организации (предприятия), в целях обеспечения их сохранности подшиваются, как правило, в дело сразу, до получения ответов на них.

Планы и отчеты помещаются в дела года, к которому они относятся, независимо от времени их составления. Перспективные планы помещаются в дела начального года действия планов, отчеты об их выполнении — в дела последнего года действия отчетов.

Листы ознакомления с распорядительными документами и листы рассылки к документам помещаются вслед за соответствующими документами, нумеруются и вносятся в описи документов дел как самостоятельные документы.

Каждое дело должно содержать, как правило, не более 250 листов. При большем количестве листов заводятся в последовательности тома дела, которые должны иметь один и тот же индекс (номер) и заголовок.

Формирование дел производится путем подшивки документов в обложки. Дела постоянного и долговременного сроков хранения должны иметь твердые обложки.

Отдельные дела могут формироваться в папках-скоросшивателях, если это не противоречит интересам обеспечения

режима конфиденциальности. Такие дела пользователям не выдаются (при необходимости могут выдаваться отдельные документы дел), в них ведется опись документов, которая по окончании года или перед сдачей дел на архивное хранение подшивается в обложку вместе с документами дела.

После подшивки изданного документа в журнале учета изданных документов проставляются индекс (номер) дела, его том и номера листов дела (тома). После подшивки поступившего документа аналогичные записи производятся в журнале учета поступивших документов.

Если в дела подшиваются документы, зарегистрированные по учетам предшествующего или следующего года (планы, отчеты и др.), то в журналах их учета рядом с индексом (номером) дела в скобках проставляется год дела, в которое они помещены.

Изъятие по каким-либо причинам документов из дела производится с разрешения руководителя подразделения конфиденциального делопроизводства, а при направлении их другим адресатам — руководителя организации (предприятия). Вместо изъятых документов в дело помещается справка-заместитель.

О документах, изъятых из дела безвозвратно, производится, кроме того, соответствующая отметка в описи документов дела. При необходимости вместо изъятых документов в дело могут быть подшиты их копии, в этом случае справка-заместитель не требуется. Отметки о снятии копий и местонахождении подлинников производятся лишь в соответствующих учетных формах документов.

Справка-заместитель (на листе формата А5) имеет следующую форму.

СПРАВКА-ЗАМЕСТИТЕЛЬ	
Документ № _____	от _____ на _____ л.
	<i>(года документа) (цифра)</i>
из дела изъят и _____	
<i>(указывается новое местонахождение документа: №№ дела и листов, или куда направлен, № и дата сопроводительного документа, или № и дата акта об уничтожении, или № по учету выделенного хранения)</i>	
Основание: _____	
_____ <i>(подпись, инициалы и фамилия лица, изъявшего документ)</i>	
« » _____	20 г.

Оформление конфиденциального дела включает в себя заполнение реквизитов дела на обложке, проставление на внутренней стороне обложки фамилий и инициалов лиц, допущенных к делу, заведение карточки учета выдачи дела, заполнение описи документов дела, нумерацию листов, составление заверительной надписи, прошивку и опечатывание дела.

Определение состава лиц, допущенных к каждому конкретному делу, должно осуществляться в соответствии с принципами и нормами системы доступа к конфиденциальным документам и исключать необоснованный доступ пользователей к делам. Указанную запись осуществляет руководитель структурного подразделения, для которого заведено это дело, заверяя ее своей подписью, например: «Дело разрешается выдавать: (перечисляются фамилии и инициалы сотрудников своего подразделения, допущенных к делу), подпись, дата». Если к делу допускаются сотрудники разных подразделений, то такую запись делает вышестоящий руководитель. Ограничение перечня лиц, допущенных к делу, не означает, что другие исполнители (не включенные в список) не имеют права направлять туда исполненные документы. Однако в этом случае запись о направлении документа в это дело, как правило, производит руководитель подразделения.

При заведении дела на обложке указываются:

- гриф конфиденциальности дела;
- название организации (предприятия);
- название структурного подразделения (если в дело помещаются документы одного структурного подразделения);
- индекс (номер) дела;
- заголовок дела;
- дата заведения (год);
- срок хранения и номера статей по перечню документов с указанием сроков хранения.

Эти же данные проставляются на обложках учетных журналов. Кроме того, на обложках учетных журналов при заведении проставляется количество имеющихся в них листов.

На обложках дел, подлежащих архивному хранению, предусматривается место для реквизитов, связанных с оформлением дела для передачи на архивное хранение.

В течение года на обложке может проставляться номер тома (при заведении второго тома номер тома проставляется и на втором, и на первом томах дела; если дело одностомное, номер тома не указывается).

При закрытии дела на обложке проставляются:

- крайние даты документов дела, которые должны соответствовать датам издания (подписания, утверждения) или поступления самого раннего и самого позднего документов, вне зависимости от расположения этих документов в деле;
- количество листов (с учетом литерных и пропущенных номеров листов, но без листов описи документов дела).

Кроме того, при закрытии дела уточняются заголовок и срок хранения дела с внесением состоявшихся изменений на обложку дела и в номенклатуру дел.

Надписи на обложках должны производиться четко, светостойкими чернилами или черной тушью.

При заведении дела в него подшиваются приблизительно необходимое количество листов внутренней описи документов дела (формат А4), следующей формы.

Внутренняя опись документов дела № _____ том № _____

Порядковый № записи	№ и гриф конфиденциальности поступившего документа	№ и гриф конфиденциальности издания документа	Дата документа	Заголовок документа, откуда поступил или кому адресован	№№ листов дела	Отметка об изъятии
1	2	3	4	5	6	7

Итого _____ документов.

(цифрами и прописью)

Количество листов в описи _____

(цифрами и прописью)

(подпись, инициалы и фамилия лица, составившего опись)

Графы 2 и 3 могут быть объединены.

Данные о документах вносятся в опись в момент подшивки документов. При подшивке в конфиденциальные дела открытых документов в графах 2 или 3 производится отметка «н/к». Если в дело подшивается документ, имеющий приложения, в том числе открытые, то запись в графах 2 или 3 производится одной позицией за номером основного документа без отметок о наличии приложений с проставлением в графе 6 номеров общего количества листов, включая листы приложений. Если документ внутренний, то в графе 5 указывается только его наименование.

Листы дела нумеруются (за исключением листа с заверительной надписью). Нумерация листов дела производится при подшивке документа арабскими цифрами черным графитовым карандашом в правом верхнем углу листа без затрагивания текста документа. Если дело имеет несколько томов, нумерация листов производится по каждому тому отдельно.

Листы описи документов дела нумеруются отдельно при начале заполнения каждого листа, оставшиеся чистые листы не нумеруются.

Лист любого формата, подшитый за один край, нумеруется как один лист, сложенный и подшитый за середину — как два листа. Подклеенные к листу одним краем другие документы (вырезки, вставки текста, переводы и т. д.) нумеруются отдельно вслед за листом основного документа; лист с наглухо наклеенными документами и фотографиями нумеруется как один лист, в этом случае наклеенные документы оговариваются в заверительной надписи.

Подшитые в дело как самостоятельные листы фотографии и другие иллюстрированные документы нумеруются при наличии свободного поля на лицевой стороне в правом верхнем углу, при отсутствии такового — на оборотной стороне в левом верхнем углу.

Подшитые в дело конверты с надписями или вложениями также нумеруются, при этом каждое вложение нумеруется очередным номером вслед за конвертом. На лицевой стороне конверта пишется опись вложенных документов с указанием их учетных номеров, краткого названия и номеров листов дела.

При изъятии документов из дел старая нумерация листов сохраняется.

При нумерации листов необходимо строго следить за ее правильностью. Однако если все же один номер окажется повторенным на нескольких листах, то следом за основным номером проставляются литерные номера, например: 10, 10а, 10б и т. д., которые оговариваются в заверительной надписи. В заверительной надписи оговариваются и пропущенные номера.

Заверительная надпись составляется при закрытии дела (на листе формата А4), по следующей форме.

Лист-заверитель дела № _____ том № _____

В деле подшито, пронумеровано и опечатано печатью № _____
 _____ лист(ов) и _____ лист(ов) внутренней описи,
 (цифрами и прописью) (цифрами)
 в том числе литерные №№ _____, пропущенные №№ _____.

Особенности физического состояния и формирования дела	№№ листов
<i>(указываются особенности документов, если они есть, например наличие наклеенных фотографий и т. п.)</i>	

(должность, подпись, фамилия и инициалы лица, оформившего заверительную надпись)
 « » _____ 20 г.

При незаполнении каких-либо позиций заверительной надписи в них делается прочерк. Незаполненные листы описи документов дела не учитываются.

Листы каждого тома дела при закрытии тома проверяются, прошиваются плотной ниткой в четыре прокола и опечатываются (аналогично опечатыванию пакетов с конфиденциальными документами). Если дела переплетаются, то их опечатывание не производится. Опечатывание конфиденциальных дел целесообразно производить при подготовке их к сдаче в архив.

Глава XII

ПОДГОТОВКА КОНФИДЕНЦИАЛЬНЫХ ДЕЛ И ДОКУМЕНТОВ ДЛЯ АРХИВНОГО ХРАНЕНИЯ ИЛИ УНИЧТОЖЕНИЯ

По истечении определенного времени дальнейшее содержание закрытых (законченных) дел и документов в подразделении конфиденциального делопроизводства становится нецелесообразным.

Вместе с тем некоторые из этих дел и документов содержат важную информацию (например, по кадровым вопросам, о деятельности государственных или муниципальных органов власти) или представляют собой историческую, научную, социальную, экономическую, политическую, культурную ценность и в связи с этим должны передаваться для архивного хранения.

Другие документы просто утрачивают со временем свое практическое значение и подлежат уничтожению (за ненадобностью).

Состав государственных и муниципальных органов власти и подведомственных им предприятий, передающих документы постоянного хранения в государственные архивы, а также категории передаваемых ими документов (все документы постоянного хранения или часть из них), определяются Федеральным архивным агентством и органами управления архивным делом субъектов Российской Федерации. В отношении негосударственных предприятий такое определение производится архивными учреждениями совместно с собственниками документов и оформляется договором.

Документы, составляющие коммерческую или служебную тайну государственных и негосударственных организаций, могут передаваться в государственные архивы с соответствующими грифами конфиденциальности (при

этом оговариваются особые условия хранения передаваемых документов и пользования ими), но на практике такая передача осуществляется обычно при ликвидации организации (предприятия) с отсутствием правопреемника. Если таких ситуаций не возникает, то документы целесообразно передавать в государственные архивы, как правило, после снятия с них грифа конфиденциальности.

Конфиденциальные документы, подлежащие передаче в государственные архивы, до их фактической передачи должны храниться соответствующим образом оформленными в архивах организаций (предприятий), а при отсутствии архивов — в подразделениях конфиденциального делопроизводства. По решению вышестоящих организаций такие документы могут передаваться в архивы этих организаций (предприятий).

В таком же порядке необходимо хранить до их уничтожения и документы, не подлежащие передаче в государственные архивы. При этом во всех случаях должны быть обеспечены условия для физической сохранности документов и предотвращения разглашения содержащейся в них информации.

С целью уточнения или определения сроков хранения документов и их отбора для архивного хранения и уничтожения проводится экспертиза ценности документов. Проведение такой экспертизы возлагается на экспертную комиссию.

Экспертиза ценности конфиденциальных дел и документов проводится по мере необходимости (ежегодно, раз в несколько лет). Экспертизой должны быть охвачены все конфиденциальные дела и документы выделенного хранения за соответствующий период времени, поскольку документы выделенного хранения являются составной частью документального фонда организации (предприятия).

Экспертиза ценности документов дела проводится путем изучения содержания каждого подшитого в дело документа и установления его соответствия сроку хранения и номерам статей перечня, указанным на обложке дела. Одновременно проверяется правильность формирования дела: соответствие видов и содержания документов заголовку дела, отсутствие в делах постоянного срока хранения документов временного срока хранения.

Экспертиза ценности документа выделенного хранения проводится путем изучения его содержания. Одновременно устанавливается возможность снятия грифа конфиденциальности с документов выделенного хранения, отдельных документов дела или с дела в целом и определения дальнейших сроков их хранения.

При определении или уточнении сроков хранения документов необходимо руководствоваться «Перечнем типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения»¹.

При проведении экспертизы ценности научно-технических документов необходимо использовать «Перечень научно-технической документации, подлежащей приему в государственные архивы России»².

Если в организации (на предприятии) имеются документы, не предусмотренные названными перечнями и методическими рекомендациями, то срок их хранения следует устанавливать на основе определенных критериев оценки документов, к важнейшим из которых относятся:

- содержание документа (значимость отображенного события, полнота его освещения, новизна, уникальность информации или ее повторяемость, целевое назначение документа);
- происхождение документа (место и время издания);
- внешние особенности документа (подлинник или копия, характер резолюций, физическое состояние).

Срок хранения дела в целом устанавливается по наименьшему сроку хранения документов, находящихся в деле.

По завершении экспертизы всех дел и документов выделенного хранения результаты работы рассматриваются экспертной комиссией и фиксируются в протоколе с отражением:

- какие дела и документы выделенного хранения (с уточненными заголовками, грифами конфиденциальности, сроками хранения и номерами статей по перечню) подлежат передаче на архивное хранение;
- какие дела, документы из дел и документы выделенного хранения подлежат уничтожению;

¹ В редакции решения Росархива 2003 г.

² Утверждены решением Росархива 1998 г.

- с каких дел, документов выделенного хранения или отдельных документов, подшитых в дела, должен быть снят гриф конфиденциальности с указанием в последнем случае, подлежит ли документ, с которого снимается гриф конфиденциальности, изъятию из дела или должен оставаться в нем.

Порядок экспертизы документов (дел) разрабатывается в организации (на предприятии) применительно к «Типовому положению о Центральной экспертной комиссии (ЦЭК) федерального органа исполнительной власти»¹.

В соответствии с утвержденным руководителем организации (предприятия) протоколом экспертной комиссии сотрудниками подразделения конфиденциального делопроизводства производится частичное реформирование и дооформление соответствующих дел и документов выделенного хранения, в том числе:

- изъятие из дел документов, подлежащих перешивке в другие дела, и подшивка их в эти дела с проставлением во внутренних описях дел, из которых изъяты документы, отметок о их новом местонахождении и помещением в дела справок-заместителей, а также с перенумерацией листов перешитых документов в делах, в которые они помещены, внесением их во внутренние описи дел и исправлением количества листов в заверительной надписи дел, на обложках дел и в номенклатуре;
- изъятие из дел документов, подлежащих уничтожению с помещением в дела справок-заместителей;
- зачеркивание грифа конфиденциальности с проставлением даты и номера протокола экспертной комиссии и заверительной подписи на документах, подшитых в дела, обложках дел и документах выделенного хранения, с которых снимается гриф конфиденциальности; во внутренних описях дел гриф конфиденциальности зачеркивается без ссылки на протокол экспертной комиссии;
- изъятие из дел документов, с которых снят гриф конфиденциальности (по решению экспертной комис-

¹ Утверждено приказом Минкультуры России 2006 г. № 35.

- передача их по акту в подразделение открытого делопроизводства с отметкой во внутренних описах дел и помещением в дела справок-заместителей;
- передача дел и документов выделенного хранения, с которых полностью снят гриф конфиденциальности, по акту в подразделение открытого делопроизводства с отметкой в номенклатуре дел или в журнале учета документов выделенного хранения;
- корректировка заголовков, сроков хранения и номеров статей по перечню на обложках дел и в номенклатуре (на обложках дел дополнительно — крайних дат документов);
- переоформление обложек и проставление сроков хранения и номеров статей перечня на обложках документов выделенного хранения.

Если срок хранения дел и документов выделенного хранения установлен не перечнем, а экспертной комиссией, то вместо статей перечня проставляется отметка «ЭК».

После изъятия из дел документов листы дела не перенумеровываются. На обложках дел и в номенклатуре рядом с количеством проставленных листов в скобках указывается количество листов, оставшихся в деле. В заверительной надписи дела под прежней надписью пишется « листов изъято согласно записям в описи дела» с проставлением заверительной подписи.

На дела и документы выделенного хранения, отображенные на архивное хранение, составляются отдельные по видам тайны описи по форме установленной Федеральным архивным агентством.

На научно-техническую, проектную, конструкторскую и иную специальную документацию составляются отдельные описи документов.

На обложках дел и документов выделенного хранения проставляются номера фонда, описи и единицы хранения.

Требования к оформлению дел и документов, а также описей для дел и документов, передаваемых на архивное хранение, изложены в «Типовой инструкции по делопроизводству в федеральных органах исполнительной власти»¹.

¹ Утверждена приказом Минкультуры России 2005 г. № 536.

Гриффы конфиденциальности описей дел должны соответствовать совокупной степени конфиденциальности сведений, содержащихся в заголовках дел и документов выделенного хранения. Если эти сведения не являются конфиденциальными, то гриффы конфиденциальности описям не присваиваются. При наличии гриффов описи регистрируются в журнале учета изданных документов.

Один экземпляр описи с подписью сотрудника архива за полученные документы передается на постоянное хранение в подразделение конфиденциального делопроизводства.

После утверждения описи дел и документов постоянного срока хранения составляется акт о выделении дел и документов за соответствующий период к уничтожению. Акт имеет форму, представленную на с. 107.

В акт включаются отобранные экспертной комиссией для уничтожения дела, отдельные документы из дел и документы выделенного хранения. Гриффы конфиденциальности акта должны соответствовать совокупной степени конфиденциальности сведений, содержащихся в заголовках дел и документов. Если эти сведения не являются конфиденциальными, то гриффы акту не присваиваются. При наличии гриффа акт регистрируется в журнале учета изданных документов.

Часть документов выделенного хранения (лишние экземпляры, справочно-информационные, присланные для сведения, отмененные), журналы (карточки) учета носителей, изданных документов, поступивших документов могут включаться в акт без рассмотрения экспертной комиссией по мере истечения установленных для них сроков хранения.

Таким же порядком уничтожаются и другие документы (носители), не подлежащие хранению. По носителям (рабочим тетрадям, отдельным учетным листам и др.) решение об уничтожении принимают пользователи этими носителями или руководители соответствующих подразделений.

Каждое дело, каждый документ и учетный журнал (карточка) вносятся в акт отдельной позицией и должны соответствовать данным о них, зафиксированным в протоколе экспертной комиссии и учетных формах. Если дело состоит из нескольких томов, то каждый из них включается в акт отдельной позицией, а в графе 3 акта пишется:

Вариант акта на уничтожение дел и документов

Наименование организации
(предприятия)

Гриф конфиденциальности
(при необходимости)

АКТ

УТВЕРЖДАЮ

о выделении к уничтожению
конфиденциальных дел
и документов

(должность руководителя
организации)

№ _____

(подпись, инициалы и фамилия)

« » _____ 20 г.

Поряд- ковый №	№ (ин- декс) дела или до- кумента и гриф кон- фиденци- альности	Заголо- вок дела или до- кумента	Год дела или доку- мента	№№ экзем- пляров доку- мента	Кол-во листов в деле или эк- земпля- ре доку- мента	Срок хране- ния и №№ статей по пер- ечню	При- меча- ние
1	2	3	4	5	6	7	8

Вариант акта на уничтожение дел и документов

Всего подлежит уничтожению _____ дел и документов.
(прописью)

(подписи, инициалы и фамилии)

Проверка правильности включения в акт дел и документов проведена.

(подписи, инициалы и фамилии)

СОГЛАСОВАНО

Протокол ЭК от « » _____ 20 г. № _____

Председатель ЭК _____
(подпись, инициалы и фамилия)

« » _____ 20 г.

Дела и документы полностью уничтожены путем _____

(подписи, инициалы и фамилии)

« » _____ 20 г.

Отметки об уничтожении дел и документов в номенклатуре дел, журнале учета документов выделенного хранения и в описях дел произведены.

(подпись, инициалы и фамилия)

« » _____ 20 г.

Гриффы конфиденциальности описей дел должны соответствовать совокупной степени конфиденциальности сведений, содержащихся в заголовках дел и документов выделенного хранения. Если эти сведения не являются конфиденциальными, то гриффы конфиденциальности описям не присваиваются. При наличии гриффов описи регистрируются в журнале учета изданных документов.

Один экземпляр описи с подписью сотрудника архива за полученные документы передается на постоянное хранение в подразделение конфиденциального делопроизводства.

После утверждения описи дел и документов постоянного срока хранения составляется акт о выделении дел и документов за соответствующий период к уничтожению. Акт имеет форму, представленную на с. 107.

В акт включаются отобранные экспертной комиссией для уничтожения дела, отдельные документы из дел и документы выделенного хранения. Гриф конфиденциальности акта должен соответствовать совокупной степени конфиденциальности сведений, содержащихся в заголовках дел и документов. Если эти сведения не являются конфиденциальными, то гриф акту не присваивается. При наличии грифа акт регистрируется в журнале учета изданных документов.

Часть документов выделенного хранения (лишние экземпляры, справочно-информационные, присланные для сведения, отмененные), журналы (карточки) учета носителей, изданных документов, поступивших документов могут включаться в акт без рассмотрения экспертной комиссией по мере истечения установленных для них сроков хранения.

Таким же порядком уничтожаются и другие документы (носители), не подлежащие хранению. По носителям (рабочим тетрадам, отдельным учетным листам и др.) решение об уничтожении принимают пользователи этими носителями или руководители соответствующих подразделений.

Каждое дело, каждый документ и учетный журнал (карточка) вносятся в акт отдельной позицией и должны соответствовать данным о них, зафиксированным в протоколе экспертной комиссии и учетных формах. Если дело состоит из нескольких томов, то каждый из них включается в акт отдельной позицией, а в графе 3 акта пишется:

Вариант акта на уничтожение дел и документов

Наименование организации
(предприятия)

Гриф конфиденциальности
(при необходимости)

АКТ

УТВЕРЖДАЮ

о выделении к уничтожению
конфиденциальных дел
и документов

(должность руководителя
организации)

№ _____

(подпись, инициалы и фамилия)

« » _____ 20 г.

Поряд- ковый №	№ (ин- декс) дела или до- кумента и гриф кон- фиденци- альности	Заголо- вок дела или до- кумента	Год дела или доку- мента	№№ экзем- пляров доку- мента	Кол-во листов в деле или эк- земпляр- е доку- мента	Срок хране- ния и №№ статей по пер- ечню	При- меча- ние
1	2	3	4	5	6	7	8

Вариант акта на уничтожение дел и документов

Всего подлежит уничтожению _____ дел и документов.
(прописью)

(подпись, инициалы и фамилия)

Проверка правильности включения в акт дел и документов проведена.

(подпись, инициалы и фамилия)

СОГЛАСОВАНО

Протокол ЭК от « » _____ 20 г. № _____

Председатель ЭК _____

(подпись, инициалы и фамилия)

« » _____ 20 г.

Дела и документы полностью уничтожены путем _____

(подпись, инициалы и фамилия)

« » _____ 20 г.

Отметки об уничтожении дел и документов в номенклатуре дел, журнале учета документов выделенного хранения и в описях дел произведены.

(подпись, инициалы и фамилия)

« » _____ 20 г.

«То же, т. _____», с добавлением номера тома. При внесении в акт дел, из которых перед уничтожением были изъяты отдельные документы, в графе 6 указывается оставшееся в деле количество листов.

Перед уничтожением включенных в акт дел, документов и учетных журналов (карточек) проверяется соответствие данных акта записям в протоколе экспертной комиссии, номенклатуре дел, журнале учета документов выделенного хранения, на обложках и в заверительных листах дел и документов выделенного хранения, в описях документов дела (по документам, изъятым из дела). Листы и учетные карточки просчитываются, сложенные документы разворачиваются. Соответствие данных заверяется в акте подписями проверявших.

Уничтожение дел, документов и учетных журналов (карточек) должно производиться с помощью бумагорезательных технических средств или сжиганием. При уничтожении документов вне территории организации (предприятия) доставка их к месту уничтожения производится на служебном транспорте и принимаются меры, исключающие доступ к документам посторонних лиц.

После уничтожения производятся отметки об уничтожении дел и учетных журналов (карточек) в номенклатуре дел, документов выделенного хранения в журнале учета документов выделенного хранения. Отметки об уничтожении отдельных документов из дел проставляются во внутренних описях документов дел.

Составление акта о выделении к уничтожению дел и документов и проставление в учетных формах отметок об их уничтожении осуществляются сотрудником подразделения конфиденциального делопроизводства.

В проверке правильности включения в акт дел и документов, а также в их физическом уничтожении должно участвовать не менее двух членов комиссии (сотрудников конфиденциального делопроизводства).

Необходимо иметь в виду, что в процессе уничтожения документов существуют угрозы (риски) конфиденциальности информации. К таким угрозам, например, относятся:

- выделение к уничтожению документов (уничтожение документов), не подлежащих уничтожению;

Подготовка конфиденциальных дел и документов...

- подмена документов, выделенных к уничтожению;
- фиктивное уничтожение документов;
- не полное уничтожение документов, позволяющее восстановить содержащуюся в них информацию;
- ознакомление с документами посторонних лиц.

Эти угрозы могут носить случайный или умышленный характер, но в любом случае необходимо принять исчерпывающие меры по недопущению реализации этих угроз.

РЕЖИМ СОХРАННОСТИ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

Организация хранения конфиденциальных документов предполагает, что помещения подразделения конфиденциального делопроизводства, должны соответствовать требованиям технической безопасности, противопожарной безопасности, а также установленным санитарным нормам.

Для обеспечения физической сохранности конфиденциальных документов, дел и носителей, а также для предотвращения разглашения содержащейся в них информации в организации (на предприятии) должен быть установлен специальный режим их хранения и обращения. Рассмотрим составляющие этого режима.

В целях обеспечения дополнительных гарантий от проникновения посторонних лиц эти помещения (по возможности) должны размещаться не на первом и последнем этажах зданий, а их окна — выходить на внутреннюю территорию объекта.

Право прохода в такие помещения имеют руководитель организации (предприятия) и сотрудники, имеющие прямое отношение к обработке и хранению конфиденциальных документов. Лица, обеспечивающие техническое и бытовое обслуживание (уборку, ремонт оборудования и технических средств), допускаются в эти помещения только в присутствии сотрудников подразделения конфиденциального делопроизводства.

Окна помещений должны иметь надежные средства защиты, исключающие возможность проникновения посторонних лиц. Кроме того, на окнах должны быть защитная сетка или жалюзи, предотвращающие возможность выпадения документов при открытых окнах, а также визуального просмотра документов и экранов видеомонито-

ров компьютеров с улицы. Если помещения расположены на первом или последнем этаже здания или рядом с ними находятся пожарные лестницы, балконы, водосточные трубы, какие-либо пристройки, с которых можно проникнуть в помещения, окна дополнительно защищаются расщепленной металлической решеткой с замком.

Входные двери помещений должны быть обиты металлическим листом и оборудованы замками, гарантирующими их надежное закрытие. По окончании рабочего дня двери необходимо не только запирают, но и опечатывают номерной металлической печатью подразделения (или сотрудника) конфиденциального делопроизводства.

Для опечатывания используются специальные устройства. Печать проставляется на тонкий слой пластилина (специальной мастики), закрывающий металлический стержень или толстую нить в специальном углублении устройства таким образом, чтобы оттиск невозможно было повредить при открывании (или, повредив, восстановить). Перед отпиранием двери проверяется сохранность оттиска печати и целостность самой двери. При обнаружении попыток проникновения в помещение нужно немедленно поставить в известность службу безопасности (охрану) и доложить руководителю организации (предприятия). При этом самостоятельно помещения не вскрываются, они обеспечиваются физической охраной до принятия соответствующего решения.

Входные двери, окна помещений (а в некоторых случаях — сейфы и шкафы) необходимо оснастить сигнализацией, связанной с дежурным постом службы безопасности (охраны). Целесообразно также оснастить эти помещения датчиками движения.

Для предотвращения несанкционированного входа в помещения в течение рабочего дня на дверях могут устанавливаться кодовые (электромеханические, электронные) замки и электрические звонки.

Для выдачи конфиденциальных документов исполнителям (пользователям), помещения должны внутри отгораживаться барьером или оборудоваться специальными окошками, не выходящими в общий коридор.

Помещения, в которых для фиксации, обработки, хранения, воспроизведения и передачи конфиденциальной до-

кументной информации используются средства вычислительной техники (ЭВМ), множительные аппараты, средства аудио-, видеозаписывающей и воспроизводящей техники, другие технические средства (в том числе радиоприемники, телевизоры), создающие электромагнитные излучения, необходимо оборудовать дополнительными средствами защиты, предотвращающими перехват таких сигналов.

В этих же целях целесообразно приобретать сертифицированные технические средства обработки информации, отвечающие требованиям по защите информации, а средства иностранного производства предварительно подвергать специальным проверкам (в уполномоченных организациях) для выявления в них возможных электронных (программных) средств технической разведки.

Конфиденциальные документы должны храниться в сейфах или металлических шкафах подразделения конфиденциального делопроизводства, которые по окончании рабочего дня должны запираются и опечатываться сотрудниками, ответственными за их учет и сохранность. В том случае, когда исполнителям разрешено работать с документами на своих рабочих местах, эти документы могут храниться в специальных портфелях, имеющих приспособление для опечатывания. По окончании рабочего дня спецпортфели, опечатанные померной печатью исполнителя, сдаются в подразделение конфиденциального делопроизводства (без проверки или списания документов) и хранятся там на металлических стеллажах.

Хранение открытых документов вместе с конфиденциальными допускается только в случаях, когда они являются приложениями к конфиденциальным документам.

Исполнители могут работать с конфиденциальными документами или в специально выделенных помещениях подразделения конфиденциального делопроизводства, или в своих служебных комнатах, если эти комнаты отвечают требованиям обеспечения конфиденциальности информации. При работе с документами в служебных комнатах каждый исполнитель должен иметь постоянное рабочее место, сейф (металлический шкаф) или отдельную ячейку сейфа для хранения конфиденциальных документов и померную металлическую печать. В этом случае исполнителю может также выдаваться спецпортфель для хранения доку-

ментов. Ключи от сейфа, спецпортфель и номерная печать выдаются исполнителю под роспись в лицевом счете (журнале учета). Номерная печать хранится у исполнителя постоянно и не должна передаваться другим лицам.

Замки дверей помещений, распашных металлических решеток на окнах, сейфов и шкафов должны иметь рабочие (первые) и запасные (вторые) экземпляры ключей. В случае утраты рабочих или запасных экземпляров ключей об этом немедленно ставятся в известность руководители организации (предприятия) и службы безопасности (охраны), а также производится немедленная замена замков. При утрате ключа от сейфа или шкафа до замены замка или смены секрета замка хранить документы в этом сейфе (шкафу) запрещено.

Вторые экземпляры ключей хранятся в опечатанных номерной печатью пеналах (конвертах) в подразделении конфиденциального делопроизводства или в службе безопасности (на одном из постов охраны). Место хранения и факт передачи запасных ключей на хранение строго регламентируются (с записью в специальном журнале).

Первые экземпляры ключей от сейфов, шкафов, решеток в нерабочее время могут храниться в опечатанном номерной печатью пенале (конверте), либо на одном из постов охраны, либо в сейфе (шкафу) у руководителя подразделения, или в подразделении конфиденциального делопроизводства. В случае хранения рабочих ключей в сейфе не на посту охраны, по окончании рабочего дня ключ от этого сейфа вместе с рабочим экземпляром ключа от входной двери помещения передается в опечатанном номерной печатью пенале на пост охраны, с записью в журнал передачи под охрану помещений и пеналов с ключами. Место хранения и факт передачи рабочих ключей от сейфов (шкафов) исполнителей на временное хранение строго регламентируются (с записью в специальном журнале или с обменом на соответствующий жетон).

Журнал передачи под охрану помещений и пеналов с ключами от этого помещения имеет форму, представленную на с. 114.

При сдаче помещений и пеналов с ключами заполняются графы 1 – 7, при получении пенала от сотрудника охраны заполняются графы 9 – 10. В графе 11 делаются

Журнал передачи под охрану помещений и пеналов с ключами

№ сдаваемого помещения	Дата и время передачи под охрану	№ печати, которой опечатано помещение	№ печати, которой опечатан пенал с ключами	Подпись лица, передавшего помещение и пенал под охрану	Отметка о включении сигнализации
1	2	3	4	5	6
<i>Продолжение</i>					
Подпись лица, принявшего помещение и пенал под охрану	Дата и время получения пенала с ключами	Подпись лица, получившего пенал	Отметка о включении сигнализации	Примечание	
7	8	9	10	11	

записи (отметки) о фактах нарушения стандартного режима охраны (о срабатывании сигнализации, нарушении целостности печатей и т. д.).

Сдача помещений и пеналов с ключами, получение пеналов, вскрытие пеналов и помещений должны осуществляться только уполномоченными сотрудниками. Список таких лиц (с указанием в нем номеров печатей и образцами подписей этих лиц), по каждому помещению, должен находиться на посту охраны.

Для вскрытия помещений без указанных лиц назначается комиссия в составе не менее двух человек, которая составляет акт о вскрытии с указанием в нем должностей и фамилий лиц, вскрывших помещения, номера помещения, времени и причины вскрытия, номеров печатей, которыми ранее были опечатаны и вновь опечатаны помещения.

Комиссионно, с составлением акта, вскрываются также сейфы, шкафы и спецпортфели при отсутствии сотрудника, ответственного за хранение находящихся в них документов. При этом в акте отражается факт изъятия документов (с проверкой соответствия фактического наличия изымаемых документов учетным данным, а также указанием учетного номера и количества листов каждого изымаемого документа) или их не изъятия. Изъятые документы списываются с исполнителя в учетных формах.

При таком вскрытии опечатывание сейфа (помещения) и запасных ключей от них производится печатями разных членов комиссии. В организациях (на предприятиях) с большим количеством сотрудников, имеющих право оставлять конфиденциальные документы у себя в сейфе (спецпортфеле), целесообразно завести журнал учета вскрытия сейфов (спецпортфелей) вместо составления разовых актов.

После прибытия на рабочее место сотрудник, у которого вскрывался сейф (спецпортфель), осуществляет его вскрытие и проверку в присутствии одного из членов комиссии, после чего расписывается в соответствующих графах журнала (в акте). Одновременно он заново опечатывает запасные ключи (второй экземпляр) от сейфа своей печатью.

Все сейфы и шкафы, установленные в помещениях подразделения конфиденциального делопроизводства и в служебных комнатах исполнителей, в которых круглосуточно

или в рабочее время хранятся конфиденциальные документы, а также ключи от них должны учитываться подразделением конфиденциального делопроизводства по журналу учета хранилищ и ключей от них, имеющим следующую форму.

Журнал учета хранилищ и ключей от них

Порядковый №	Наименование изделия	Заводской № изделия	Местонахождение	Фамилия и инициалы ответственного за изделие	Количество экземпляров ключей и их номера	Подпись за получение ключей, дата	Подпись за возврат ключей, дата
1	2	3	4	5	6	7	8

При внесении в журнал данных о ключах от металлических решеток графа 3 не заполняются.

Ежегодно должна проводиться проверка фактического наличия ключей от хранилищ и номерных печатей исполнителей.

Для эвакуации конфиденциальных документов при возникновении стихийных бедствий, пожара, аварии, грозящих уничтожением (порчей) документов, в помещениях, предназначенных для их хранения, должно находиться необходимое количество специальной тары (опечатываемых мешков, чемоданов, контейнеров).

При возникновении чрезвычайной ситуации сотрудники конфиденциального делопроизводства должны немедленно вызвать соответствующую аварийную службу, уведомить охрану, руководителя организации (предприятия), принять меры к ликвидации чрезвычайной ситуации, а также обеспечить охрану документов (собственными силами и силами охраны) и начать эвакуацию документов в заранее определенное охраняемое место.

При возникновении чрезвычайной ситуации в нерабочее время проведение аналогичных действий должен организовать дежурный сотрудник охраны, дополнительно поставив в известность руководителя подразделения конфиденциального делопроизводства. О проведенном вскрытии (при необходимости) помещений, а также о вскрытии по согласованию с руководителем организации или подразделения конфиденциального делопроизводства сейфов и шкафов составляется акт (комиссионно).

Действия персонала при различных видах угроз и непосредственно в экстремальных ситуациях должны быть прописаны в соответствующих инструкциях. Персонал подразделения конфиденциального делопроизводства и сотрудники охраны должны на практике отработать эти вопросы и научиться взаимодействию. При проведении практических занятий одновременно фиксируется время выполнения тех или иных действий для оптимизации принимаемых решений. (Например, необходимо четко знать время подготовки и эвакуации всех документов или наиболее ценных; необходимое количество дополнительно выделяемых сотрудников и из каких они подразделений; маршруты эвакуации; силы и средства, выделяемые для охраны; расчетное время прибытия аварийных служб и т. д.)

Второй составляющей режима сохранности конфиденциальных документов является строгий порядок обращения с ними. Регламентация обращения с конфиденциальными документами предполагает реализацию определенных системных требований.

Так, выдача конфиденциальных документов может производиться только исполнителям (пользователям), имеющим санкционированный доступ к этим документам, и только под роспись в учетных формах.

Выдача документов исполнителям и их возврат осуществляются в течение одного рабочего дня, но если исполнителям разрешено работать с конфиденциальными документами в своих служебных комнатах, то документы (кроме дел) допускается выдавать им на все время, необходимое для работы с ними. В последнем случае, помимо сейфа (с ключами и пеналом), спецпортфеля и номерной печати, исполнителю выдается (под роспись в лицевом счете) журнал (форма) описи документов. Опись имеет следующую форму.

Опись документов, находящихся у _____
(фамилия и инициалы)

Порядковый №	Дата получения документа	Учетный № и гриф конфиденциальности документа	Вид или название документа	Кол-во листов	Отметка о возврате документа
1	2	3	4	5	6

В опись исполнитель должен самостоятельно вносить каждый выдаваемый ему документ, (если этот документ не подлежит сдаче в подразделение конфиденциального делопроизводства в этот же рабочий день). После возврата документа в описи производится его списание (проставлением росписи сотрудника конфиденциального делопроизводства в графе 6). После чего производится перечеркивание (одной чертой) этой записи исполнителем.

Опись предназначена для осуществления контроля и самоконтроля исполнителя за наличием у него документов. С этой целью перед сдачей спецпортфеля с документами в подразделение конфиденциального делопроизводства исполнитель должен проверить наличие находящихся у него документов и их соответствие описи. При отсутствии каких-либо документов (отдельных страниц) немедленно организуется их поиск. После проверки документы вместе с описью помещаются в спецпортфель, который опечатывается номерной печатью исполнителя и передается в подразделение конфиденциального делопроизводства. Не допускается хранить в спецпортфеле открытые документы, если они не являются приложением к конфиденциальным документам.

Спецпортфели могут храниться у исполнителей только в течение рабочего дня. Их получение и возврат производятся в обмен на специальный жетон, удостоверение или пропуск сотрудника. При приеме спецпортфеля необходимо проверять соответствие номера и четкость оттиска печати.

Должностные лица, которым разрешено в нерабочее время хранить конфиденциальные документы в личных сейфах, по окончании рабочего дня помещают документы в сейф, опечатывают его и сдают помещение под охрану (с соответствующими записями в журнале передачи под охрану помещений и пеналов с ключами).

По завершении работы с документами исполнители должны своевременно возвращать их в подразделение конфиденциального делопроизводства.

При увольнении, уходе в отпуск, отъезде в командировку исполнители сдают в подразделение конфиденциального делопроизводства все хранящиеся в их сейфах или спецпортфелях конфиденциальные документы и носители, со списанием их в учетных формах.

Рабочее место исполнителя должно быть организовано таким образом, чтобы исключалось обозрение (в том числе и через окна) находящихся на столе конфиденциальных документов лицами, не имеющими к ним отношения.

На столе должны быть только те конфиденциальные документы, с которыми осуществляется работа. Все остальные должны находиться в запортом сейфе. Не разрешается хранение конфиденциальных документов в ящиках столов и других, не предназначенных для этого местах.

При выходе исполнителя в течение рабочего дня из служебной комнаты документы убираются в сейф. При выходе из комнаты всех исполнителей дверь комнаты должна запирается.

Крупноформатные конфиденциальные документы на чертежных досках на время отсутствия исполнителя должны закрываться специальными защитными чехлами, опечатываемыми его печатью.

Подразделение конфиденциального делопроизводства обязано осуществлять периодический контроль за порядком хранения документов в служебных комнатах исполнителей и обращения с ними.

Нарушения порядка обращения с конфиденциальными документами необходимо учитывать для последующего анализа и принятия мер по их предотвращению. Учет может осуществляться в карточке (журнале), имеющем следующую форму.

Журнал учета нарушений порядка обращения с конфиденциальными документами

Дата нарушения	Фамилия и инициалы лица, допустившего нарушения	Наименование структурного подразделения	Краткое изложение нарушения	Принятые меры, № приказа	№ и дата заключения внутреннего расследования
1	2	3	4	5	6

О серьезных нарушениях, которые привели или могли привести к утрате документов или разглашению содержащейся в них информации, подразделение конфиденциального делопроизводства должно докладывать руководителю организации (предприятия) и вносить предложения об от-

странении от работы с конфиденциальными документами или привлечении к ответственности виновных лиц.

При смене или временном отсутствии руководителя и сотрудников подразделения конфиденциального делопроизводства передача документов замещающим их лицам производится по актам или распискам с обязательной проверкой фактического наличия передаваемых документов.

Требования к режиму обращения с конфиденциальными документами должны быть закреплены в «Положении по обеспечению сохранности коммерческой (служебной) тайны организации (предприятия)». Эти требования должны доводиться под роспись до каждого сотрудника, допущенного к работе с конфиденциальными документами, как перед началом такой работы, так и периодически во время работы (первичный и периодические инструктажи).

КОНТРОЛЬ НАЛИЧИЯ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

Проверки наличия конфиденциальных документов являются важной составной частью конфиденциального делопроизводства. Цель проверок состоит в обеспечении контроля за сохранностью документов. Это достигается путем установления соответствия фактического наличия документов учетным данным, выявления отсутствующих документов и принятия мер по их поиску.

Однако и в процессе регистрации документов могут быть допущены ошибки, следствием которых становится искажение учетных данных о документах.

Зарегистрированные документы могут быть отправлены, уничтожены, подшиты в дела, возвращены после отправления, переведены на другой вид учета. При проставлении в учетных формах отметок о таком движении документов также могут случаться ошибки, которые при определенных обстоятельствах создают основу для утраты документов и (или) несвоевременного обнаружения утрат.

Поэтому проверки правильности регистрации документов и проставления отметок о их движении должны быть составными частями проверок наличия документов. Проверки направлены и на выявление неучтенных по каким-либо причинам конфиденциальных документов, установление и устранение причин этого, взятие таких документов на учет.

«Положение о порядке обращения со служебной информацией ограниченного распространения» (см. Приложение 3) предусматривает проведение проверок наличия документов не реже одного раза в год, не запрещая тем самым более частое (оптимальное для данной организации) их проведение.

Проверками должны быть охвачены не только документы, но и дела, а также носители конфиденциальной информации.

Необходимыми видами проверок являются:

- проверки правильности проставления регистрационных данных носителей, документов, дел и учетных журналов;
- проверки правильности проставления отметок о движении носителей, документов и дел;
- проверки фактического наличия всех носителей и всех не подшитых в дела и не переведенных на учет выделенного хранения изданных и поступивших документов, независимо от времени их регистрации;
- проверка фактического наличия всех дел, документов выделенного хранения и учетных журналов (картотек), зарегистрированных в истекшем и предыдущих годах.

Проверочные операции целесообразно проводить одновременно двум сотрудникам конфиденциального делопроизводства (или членам назначенной комиссии). При этом каждый из сотрудников не дублирует проверочные операции, а выполняет определенную их часть. Например, один сотрудник называет учетные данные на документе, другой проверяет их соответствие в учетных формах, или один называет данные учетных форм, другой проверяет их соответствие в других учетных формах, сопроводительных документах, делах и т. д. Это повышает качество проверок и ускоряет их проведение.

В целях обеспечения контроля за проведением всех необходимых проверочных операций и избежания их дублирования необходимо проставлять соответствующие отметки о проверках. Отметки о проверках целесообразно проставлять условным обозначением, например: «V», «+» и др. Отметки допускается производить карандашом, чтобы при необходимости можно было их убрать, с целью освобождения места для проставления последующих отметок.

Отметки о проверках фактического наличия или движения носителей, документов, дел и учетных журналов (карточек) допускается проставлять датами проверок, поскольку, как уже отмечалось, такие проверки частично повторяются и по дате можно отличить одну проверку от другой.

122 При проведении проверок необходимо обеспечить, чтобы проверочными операциями были охвачены все под-

лежащие проверке документы, дела и носители, все учетные формы, в которых зафиксированы проверяемые реквизиты, и все сопроводительные материалы о движении документов. Результаты проверок должны быть зафиксированы (в актах, в учетных формах).

Технологии проведения названных видов проверок различаются между собой, поэтому целесообразно рассмотреть их по каждому виду подробнее.

Для проверки правильности проставления регистрационных данных бумажных носителей используются журнал учета бумажных носителей и носители. В журнале и на носителе проверяется соответствие записей об учетном номере и грифе конфиденциальности носителя, дате регистрации, виде, наименовании или назначении носителя, количестве листов. В носителе проверяется правильность нумерации листов. Отметки о проверке проставляются в журнале (рядом с номерами носителей).

Если бумажные носители в момент их заведения регистрируются не в журнале учета бумажных носителей, а в журнале учета документов выделенного хранения (например, рабочие тетради), то для проверки правильности их регистрации используются журнал учета документов выделенного хранения и носители. В журнале и на носителе проверяется соответствие записей об учетном номере и грифе конфиденциальности носителя, дате регистрации, виде и наименовании носителя, наименовании подразделения (фамилии и инициалов пользователя), номерах экземпляров, количестве листов в экземпляре. В носителе проверяется правильность нумерации листов. Отметки о проверке проставляются в журнале (рядом с номерами документов).

Для проверки правильности проставления регистрационных данных машинных носителей используются журнал учета машинных носителей и носители. В журнале и на носителе проверяется соответствие вида и типа носителя, его учетного номера и грифа конфиденциальности. Отметки о проверке проставляются в журнале (рядом с номерами носителей).

Для проверки правильности проставления регистрационных данных изданных документов используются журнал учета изданных документов, документы и черновики. В журнале и на документе проверяется соответствие

записей об учетном номере, грифе конфиденциальности, дате, виде и названии документа, фамилии исполнителя (на документе — в реквизите «Отметка об исполнителе»), количестве экземпляров (в документе — по их фактическому наличию, и в реквизите «Отметка об исполнителе»), количестве листов в экземпляре. В документе проверяется правильность нумерации листов, проставление учетных номеров на каждом листе, проставление номера экземпляра на каждом экземпляре. В журнале и на черновике проверяется соответствие номера носителя и номеров листов черновика. Отметки о проверке проставляются в журнале (рядом с номерами документов).

Наиболее сложной является проверка правильности проставления регистрационных данных поступивших документов, поскольку в их состав входят документы, зарегистрированные по журналу учета поступивших документов, журналу учета документов выделенного хранения, а также возвращенные документы, которые ранее были зарегистрированы по разным видам учета.

Для проверки правильности проставления регистрационных данных поступивших документов используются журнал учета поступивших документов, реестры поступивших документов и документы. В журнале учета поступивших документов проверяется соответствие данных тем, которые указаны в реестрах. В журнале и на документе проверяется соответствие присвоенного учетного номера, грифа конфиденциальности, даты поступления, вида и названия документа, наименования отправителя, номера, за которым документ направлен, даты документа, количества листов (с просчетом их в документе). В документе, имеющем приложения, дополнительно проверяется соответствие учетных номеров, грифов конфиденциальности, номеров экземпляров, количества листов в экземпляре данным, содержащимся в реквизите «Отметка о наличии приложения». Отметки о проверке проставляются в журнале учета поступивших документов (рядом с номерами документов).

Для проверки правильности присвоения регистрационных данных поступивших документов, взятых сразу на учет, документов выделенного хранения без промежуточной регистрации их в журнале учета поступивших документов используются журнал учета поступивших документов, ре-

естры поступивших документов, журнал учета документов выделенного хранения и документы. В журнале учета поступивших документов проверяется соответствие данных тем, которые указаны в реестрах. В журнале учета документов выделенного хранения и на документе проверяется соответствие присвоенного учетного номера и грифа конфиденциальности, даты регистрации, вида и название документа, наименования отправителя, номера, за которым документ направлен, номеров экземпляров, количества листов в экземпляре (с просчетом их в каждом экземпляре). Отметки о проверке проставляются в журнале учета поступивших документов и в журнале учета документов выделенного хранения (рядом с номерами документов).

Для проверки правильности проставления отметок о возврате ранее отправленных документов используются журнал учета поступивших документов, другие необходимые журналы учета и документы. В журнале учета проверяется наличие отметки о возврате документа и ее соответствие записи в журнале учета поступивших документов. В журналах учета изданных документов, документов выделенного хранения и на документах проверяется, кроме того, соответствие номеров возвращенных экземпляров документов. Отметки о проверке проставляются в журнале учета поступивших документов (рядом с номерами возвращенных документов).

Для проверки правильности проставления отметок о возврате ранее отправленных машинных носителей используются журнал учета поступивших документов, журнал учета машинных носителей и носители. В журнале учета машинных носителей проверяется наличие отметки о возврате носителя и ее соответствие с записью в журнале учета поступивших документов. Отметки о проверке проставляются в журнале учета поступивших документов (рядом с номерами возвращенных носителей).

Для проверки правильности проставления регистрационных данных дел и учетных журналов (карточек) используются номенклатура дел, дела и учетные журналы (карточки). В номенклатуре и на обложке дела (журнала) проверяется соответствие индекса (номера) дела (журнала), грифа конфиденциальности, заголовка (наименования), срока хранения и номеров статей по перечню. По учетным журналам,

кроме того, проверяется соответствие количества листов. Отметка о проверке проставляется в номенклатуре рядом с индексом (номером) дела, журнала или карточки.

Для проверки правильности проставления отметок об отправлении документов используются учетные журналы, в которых зарегистрированы отправленные документы, и сопроводительные материалы, по которым отправлены документы (реестры, расписки, квитанции, сопроводительные письма). В журнале и сопроводительном документе проверяется соответствие записей о номере, грифе конфиденциальности, виде и названии документа, адресате, номерах отправленных экземпляров (по документам, зарегистрированным в журнале учета поступивших документов, вместо номеров экземпляров проверяется количество отправленных листов), названии, номере и дате сопроводительного документа. Подписи (отметки) о проверке проставляются в журнале учета изданных документов, в журнале учета документов выделенного хранения или в журнале учета поступивших документов.

Для проверки правильности проставления отметок о переводе изданных и поступивших документов на учет документов выделенного хранения используются журналы учета изданных, поступивших документов и документов выделенного хранения и переведенные на учет выделенного хранения документы. В журнале и документе проверяется соответствие учетного номера, присвоенного при издании или поступлении документа, учетному номеру, присвоенному по журналу учета документов выделенного хранения, грифа конфиденциальности, вида, названия и номеров экземпляров документа, количества листов в экземпляре с просчетом листов. Подписи (отметки) о проверке проставляются в журнале учета изданных документов или в журнале учета поступивших документов. В журнале учета документов выделенного хранения рядом с номером документа проставляется отметка о проверке правильности регистрации.

Для проверки правильности проставления отметок об отправлении (возврате) ошибочно присланных документов используются журнал учета поступивших документов и копии сопроводительных писем, с которыми отправлены документы. В журнале и сопроводительном письме проверяется соответствие записей о номере и грифе конфиден-

циальности документа, адресате, номере и дате сопроводительного письма. Подписи (отметки) о проверке проставляются в журнале учета поступивших документов.

Для проверки правильности проставления отметок об отправлении машинных носителей используются журнал учета машинных носителей и сопроводительные документы, с которыми отправлены носители. В журнале и сопроводительном документе проверяется соответствие записей о виде, номере, грифе конфиденциальности носителя, адресате, номере и дате сопроводительного документа. Подписи (отметки) о проверке проставляются в журнале учета машинных носителей.

Для проверки правильности проставления отметок об отправлении дел используются номенклатура дел и сопроводительные документы, с которыми отправлены дела. В номенклатуре дел и сопроводительном документе проверяется соответствие записей об индексе (номере) и грифе конфиденциальности дела, названии дела, номере тома, количестве листов в томе, адресате, номере и дате сопроводительного документа. Подписи (отметки) о проверке проставляются в номенклатуре дел.

Для проверки правильности проставления отметок об отправлении документов, изъятых из дел, используются дела, из которых изъятые документы, и сопроводительные документы, с которыми отправлены изъятые документы. В сопроводительном документе, описи документов дела и справке-заместителе проверяется соответствие записей о номере, грифе конфиденциальности и количестве листов документа, адресате, номере и дате сопроводительного документа. Подписи (отметки) о проверке проставляются в описи документов дела.

Кроме того, в процессе проверок правильности проставления отметок об отправлении в сопроводительном документе (за исключением сопроводительных писем) проверяется наличие подписи лица за получение пакетов и оттиска печати (штампа).

Для проверки правильности проставления отметок об уничтожении документов выделенного хранения используются журнал учета документов выделенного хранения и акты об уничтожении дел и документов. В журнале и акте проверяется соответствие записей об учетном номере, грифе

конфиденциальности, виде и названии документа, номерах экземпляров, количестве листов в экземпляре, номере и дате акта об уничтожении. Подписи (отметки) о проверке проставляются в журнале учета документов выделенного хранения.

Для проверки правильности проставления отметок об уничтожении дел и учетных журналов (карточек) используются номенклатура дел и акты об уничтожении дел и документов. В номенклатуре и акте проверяется соответствие записей об индексе (номере) и грифе конфиденциальности дела (журнала), его названии, номере тома, количестве листов в томе, номере и дате акта об уничтожении. Подписи (отметки) о проверке проставляются в номенклатуре дел.

Для проверки правильности проставления отметок об уничтожении документов, изъятых из дел, используются дела, из которых изъятые документы, и акт об уничтожении дел и документов. В акте, описи документов дела и справке-заместителе проверяется соответствие записей о номере, грифе конфиденциальности и дате документа, количестве листов, номере и дате акта об уничтожении. Подписи (отметки) о проверке проставляются в описи документов дела.

Кроме того, в процессе проверок правильности проставления отметок об уничтожении документов и дел в акте об уничтожении проверяется наличие отметок о физическом уничтожении документов и дел, заверенных подписями лиц, производивших уничтожение.

Для проверки правильности проставления отметок о подшивке документов в дела используются дела, в которых подшиты документы, и журналы учета, в которых зарегистрированы документы. В деле и соответствующем журнале проверяется соответствие учетного номера, грифа конфиденциальности, вида и названия документа, индекса (номера) дела, количества листов в документе, номеров листов дела. Кроме того, в описи документов дела и документе проверяется соответствие даты, номера, грифа конфиденциальности, вида и названия документа, отправителя (по поступившим документам) или адресата (по отправленным документам), номеров листов дела. Подписи (отметки) о проверке проставляются в журнале учета изданных документов или в журнале учета поступивших документов.

Для проверки правильности проставления отметок о перешивке документов в другие дела используются дела, из ко-

торых изъяты документы, и дела, в которые документы подшиты. В описи документов дела, в которое перешит документ, и на документе проверяется соответствие данных, перечисленных в предыдущем абзаце. В справке-заместителе и описи документов дела, из которого изъят документ, проверяется наличие данных о новом местонахождении документа и их соответствие данным описи документов дела, в которое подшит документ. Подписи (отметки) о проверке проставляются в описи документов дела, из которого изъят документ.

Для проверки правильности проставления отметок об изъятии из дела документов, с которых снят гриф конфиденциальности, используются дела и акт передачи документов в подразделение открытого делопроизводства. В описи документов дела, справке-заместителе и акте проверяется соответствие данных о номере, дате и количестве листов документа, дате и номере акта о передаче. Подписи (отметки) о проверке проставляются в описи документов дела.

При любом изъятии документов из дел в учетных формах, в которых документы были зарегистрированы, отметки о новом местонахождении или уничтожении документов не производятся.

Для проверки правильности проставления отметок о передаче на архивное хранение дел и документов выделенного хранения используются номенклатура дел, журнал учета документов выделенного хранения и описи дел и документов, переданных на архивное хранение. В описи и номенклатуре проверяется соответствие индекса (номера), грифа конфиденциальности, названия дела, номера тома дела, количества листов в томе, архивного шифра (номеров фонда, описи, единицы хранения). Подписи (отметки) о проверке проставляются в номенклатуре дел. В журнале учета документов выделенного хранения и описи проверяется соответствие номера, грифа конфиденциальности, вида и названия документа, номера экземпляра, количества листов в экземпляре, архивного шифра. Подписи (отметки) о проверке проставляются в журнале учета документов выделенного хранения.

Для проверки правильности проставления отметок о передаче в подразделение открытого делопроизводства дел и документов выделенного хранения, с которых снят гриф конфиденциальности, используются номенклатура

дел, журнал учета документов выделенного хранения и акт передачи. В номенклатуре и акте проверяется соответствие индекса (номера), названия дела, номера тома, количества листов, номера и даты акта. Подписи (отметки) о проверке проставляются в номенклатуре дел. В журнале учета документов выделенного хранения и акте проверяется соответствие учетного номера, вида и названия документа, номеров экземпляров, количества листов в экземпляре, номера и даты акта. Подписи (отметки) о проверке проставляются в журнале учета документов выделенного хранения.

Для проверки фактического наличия бумажных носителей, независимо от времени их регистрации, используются журнал учета бумажных носителей и носители. В журнале и на носителе проверяется соответствие учетного номера и количества листов (с подсчетом листов в носителе).

Для проверки фактического наличия машинных носителей, независимо от времени их регистрации, используются журнал учета машинных носителей и носители. В журнале и на носителе проверяется соответствие учетного номера.

Для проверки наличия не подшитых в дела и не переведенных на выделенное хранение изданных документов, независимо от времени их регистрации, используются журнал учета изданных документов и документы. В журнале и на документе проверяется соответствие учетного номера, грифа конфиденциальности, количества экземпляров документа и количества листов в каждом экземпляре с их просчетом. Одновременно проверяется наличие подписи за уничтожение черновика (если он был). Если на момент проверки по каким-либо причинам черновик не уничтожен, то проверяется его наличие с подсчетом листов и соответствием записям в журнале учета изданных документов.

Для проверки наличия не подшитых в дела и не переведенных на выделенное хранение поступивших документов, независимо от времени их регистрации, используются журнал учета поступивших документов и документы. В журнале и на документе проверяется соответствие учетного номера, грифа конфиденциальности, количества листов основного документа и приложений (при их наличии) с просчетом листов.

Даты проверок фактического наличия документов (носителей) проставляются в соответствующем журнале рядом с номерами документов (носителей).

Если к началу проверки носитель, изданный или поступивший документ сняты с учета (уничтожены, отправлены, переведены на учет документов выделенного хранения, подшиты в дела), то в форме учета проверяется наличие отметок и подписей о произведенных операциях с установлением (кроме магнитных носителей) соответствия количества зарегистрированных листов (а по изданным документам — и экземпляров) количеству снятых с учета. Учетный номер отмечается как закрытый.

Если по итогам проверки выявится отсутствие отдельных зарегистрированных документов (носителей), то должны быть приняты меры по их оперативному поиску. Одновременно назначается комиссия и проводится внутреннее (служебное) расследование, порядок проведения которого изложен в гл. XVI. Комиссия создается и при обнаружении в ходе проверок неучтенных конфиденциальных документов (носителей). Выявленные неучтенные документы регистрируются в соответствующих формах учета.

Целесообразно ежеквартально проверять наличие и движение всех зарегистрированных документов (поступивших, изданных) и носителей за истекший квартал, даже если они еще не подшиты в дела (не исполнены).

Проверка наличия дел проводится после подшивки в дела истекшего года всех поступивших и изданных за этот год документов и после закрытия дел (просчета листов, составления заверительной надписи дела, его прошивки и опечатывания). Если отдельные документы требуют длительного исполнения и поэтому не подшиты в дела, то их следует перерегистрировать в журнал учета документов следующего года с целью закрытия соответствующего дела за истекший год, (за исключением документов выделенного хранения).

Для проверки фактического наличия всех дел, зарегистрированных в истекшем и предыдущих годах, используются дела и номенклатуры дел за соответствующие годы. На обложке дела и в номенклатуре проверяется соответствие индекса (номера) дела, номера тома дела, грифа конфиденциальности дела, количества листов в томе. Кроме того, в делах, зарегистрированных в истекшем году, проверяется соответствие данных о количестве листов на обложке дела и в заверительной надписи.

Для проверки наличия всех документов выделенного хранения, зарегистрированных в истекшем и предстоящих годах, используются журнал учета документов выделенного хранения и документы. В журнале и на документах проверяется соответствие учетного номера и грифа конфиденциальности, номеров экземпляров, количества листов в экземпляре (в документе количество листов — по заверительной надписи, если не проставлено на обложке; если проставлено, то по заверительной надписи только в документах, зарегистрированных в истекшем году).

Проверка наличия учетных журналов (карточек) проводится после выверки и закрытия журналов учета носителей (при их годовом учете), изданных и поступивших за истекший год документов. В ходе выверки осуществляется проверка наличия закрытия всех регистрационных номеров (снятия носителей и документов с учета по данным регистрационным номерам). При этом если отдельные документы и носители перерегистрированы в журналы учета следующего года, то в журналах учета документов (носителей) текущего и следующего годов проверяется соответствие учетных данных, а на документе (носителе) — наличие нового учетного номера. Правильность отметок о перерегистрации в журнале текущего года заверяется подписями проверяющих, а в журнале следующего года рядом с номером документа (носителя) проставляется отметка о проверке правильности регистрационных данных. В закрываемых учетных формах после последнего регистрационного номера производится запись: «Все учетные номера закрыты и проверены», заверяемая подписями проверяющих с проставлением даты. При наличии незакрытых учетных номеров выявляются причины и принимаются меры по их закрытию.

Для проверки наличия всех учетных журналов (карточек), заведенных в истекшем и предыдущих годах, используются журналы (карточки) и номенклатура дел. В журнале и номенклатуре проверяется соответствие учетного номера и грифа конфиденциальности, номера тома (при наличии двух и более томов), количества листов (в журнале — по заверительной надписи). В карточке и номенклатуре проверяется соответствие учетного номера.

Даты проверок проставляются в номенклатуре дел рядом с индексом (номером) дела (журнала, картотеки), в

журнале учета документов выделенного хранения — рядом с номером документа. Выявление отсутствующих дел, документов и журналов производится путем выверки отметок (даг проверок и подписей) о снятии их с учета. При отсутствии дел, документов и журналов организуется их поиск, проводится внутреннее (служебное) расследование.

Результаты произведенных проверок правильности проставления отметок о регистрации и движении документов, дел, носителей и их фактического наличия отражаются в акте (актах).

В акте указываются только действительно проведенные виды проверок. Если какие-то виды проверок проводились поквартально, то в годовую проверку они не включаются (для исключения дублирования проверочных мероприятий).

При наличии заключений (материалы внутренних расследований) по фактам утрат или выявления неучтенных документов, они прилагаются к акту.

Внеплановые проверки наличия конфиденциальных носителей, документов и дел проводятся при смене руководителя и сотрудников (приеме новых сотрудников) подразделения конфиденциального делопроизводства, их временном отсутствии (болезнь, командировка, отпуск), нарушении оттисков печатей на хранилищах документов и ликвидации организации (предприятия). Они могут назначаться и в других случаях, когда для этого имеются определенные основания (по усмотрению руководителя организации или руководителя подразделения конфиденциального делопроизводства).

Во всех случаях они осуществляются путем проверки соответствия фактического наличия носителей, документов и дел учетным данным на них.

При смене руководителя подразделения конфиденциального делопроизводства проводится проверка наличия всех носителей, документов и дел, независимо от времени их регистрации. Проверка проводится комиссией, назначаемой приказом руководителя организации (предприятия). Результаты проверки отражаются в общем акте приема-передачи дел.

При смене сотрудника подразделения конфиденциального делопроизводства проводится проверка наличия носителей, документов и дел, находящихся на ответственном хранении сотрудника. Проверка осуществляется сдающим и

принимающим сотрудникам. Результаты проверки оформляются актом приема-передачи, подписываемым этими сотрудниками и утверждаемым руководителем подразделения конфиденциального делопроизводства. В случае отсутствия сменяемого сотрудника проверка проводится комиссией.

На период временного отсутствия руководителя или сотрудника подразделения конфиденциального делопроизводства, числящиеся за ними документы, носители и дела, необходимые для текущей работы, передаются замещающим их лицам по разовой расписке (при передаче отдельных документов) или по акту с проверкой соответствия их фактического наличия учетным данным. При отсутствии передающего лица проверка проводится комиссией. Носители, документы и дела, которые не требуются для работы на период временного отсутствия лица, не передаются. Они должны храниться в опечатанных металлических шкафах (сейфах). При этом составляется акт, в котором указываются номера хранилищ и номер печати, которой они опечатаны. Принимающее лицо не несет ответственности за находящиеся в этих хранилищах документы, если оттиск печати на них не будет нарушен. При нарушении оттиска печати, а также в случае проникновения в помещения, в которых хранятся носители, документы и дела, посторонних лиц со вскрытием хранилищ или нарушением оттиска печатей на них, назначается комиссия для проверки наличия находящихся в хранилищах документов и проведения внутреннего (служебного) расследования. Результаты проверки оформляются актом.

При ликвидации организации (предприятия) проверка наличия носителей, документов и дел проводится комиссией, назначаемой руководителем организации (предприятия). Результаты проверки оформляются актом, который приобщается к общему акту о ликвидации.

В организациях (на предприятиях) могут устанавливаться и другие (дополнительные) виды проверок. Например, в тех случаях, когда большому числу сотрудников разрешено работать с конфиденциальными документами в служебных комнатах, целесообразно ежемесячно (или еженедельно) проверять наличие документов у этих исполнителей в спецпортфелях. Для этого подразделение конфиденциального делопроизводства готовит выписку из учетных форм по всем документам, временно выданным каждому исполни-

телю проверяемых подразделений. Затем проверяется фактическое наличие этих документов у исполнителя. Запись о проверке делается на последнем листе описи документов, например: «Проверка произведена. Документы в наличии». Ставится подпись проверяющего лица, дата.

Вариант акта проверки

Наименование организации (предприятия)	Гриф конфиденциальности (при необходимости)
АКТ о проверке конфиденциальных дел, документов и учетных журналов за 20 ____ год, № _____	УТВЕРЖДАЮ _____ (должность, руководителя организации) _____ (подпись, инициалы и фамилия) « ____ » _____ 20 ____ г.

Составлен: _____
 (инициалы и фамилии лиц, проводивших проверку)

На основании: _____, с _____ по _____ 20 ____ г.
 (ссылка на № приказа, распоряжения, инструкции)

проведена проверка:

- правильности произведенных отметок о регистрации учетных журналов (карточек), дел, документов, носителей и их движения за истекший год;
- фактического наличия поступивших и изданных документов за истекший год (подсчетом листов);
- фактического наличия учетных журналов (карточек), дел, документов выделенного хранения и носителей, зарегистрированных за истекший и предыдущие годы (без подсчета листов)¹;
- закрытия всех регистрационных номеров в журналах (карточках) учета изданных и поступивших документов, зарегистрированных за истекший год.

В результате проверки установлено:

1. Все подлежащие проверке учетные журналы (карточки), дела, документы (поступившие, изданные, переведенные на выделенное хранение) и носители находятся в наличии².
2. Все отметки о регистрации дел, документов и носителей соответствуют сопроводительным материалам, а отметки о движении соответствуют новому местонахождению подшитых и переведенных на учет выделенного хранения документов³.
3. Все регистрационные номера в журналах (карточках) учета изданных и поступивших документов, зарегистрированных за истекший год, закрыты⁴.
4. Имеются следующие нарушения в учете и хранении дел, документов и носителей (указываются отдельно по делам, видам документов и носителей, а также меры, принятые по их устранению)⁵.

Приложения⁶.

 (подпись, инициалы и фамилия)

Примечания:

¹ Если подсчет листов производился, то это указывается.

² Если не все в наличии, то пишется: «кроме», с указанием учетных номеров документов, носителей или индексов (номеров) и года дел (журналов).

³ Если обнаружены факты несоответствия, то пишется: «кроме», с указанием по каждому документу (носителю, делу) в чем они проявились.

⁴ Если не все закрыты, то пишется «кроме», с указанием учетных номеров таких документов (дел); при закрытии журналов (карточек) учета, ведущихся несколько лет, они также указываются.

⁵ Пункт включается при выявлении ошибок и нарушений.

⁶ Приложения включаются в акт при их наличии.

В акт включаются только те виды проверочных мероприятий, которые фактически проводятся. Если какие-то виды проверок проводятся поквартально, то в годовую проверку они не включаются (для исключения дублирования проверочных мероприятий), а в наименовании акта указываются их название (кратко) и номер квартала, за который осуществляется проверка.

ПРОВЕДЕНИЕ КОНФИДЕНЦИАЛЬНЫХ СОВЕЩАНИЙ

Совещания с привлечением сотрудников различных подразделений организации (предприятия) и переговоры с представителями других организаций (предприятий), в процессе которых обсуждаются конфиденциальные вопросы, являются одним из возможных каналов разглашения конфиденциальной информации.

Во время проведения таких совещаний (переговоров) достаточно часто происходит ознакомление участников с совокупной и потому особенно ценной и актуальной конфиденциальной информацией.

Для предотвращения или существенного уменьшения возможного ущерба от ознакомления довольно широкого круга лиц с такой информацией, в «Положении о режиме коммерческой (служебной) тайны организации (предприятия)» необходимо предусмотреть порядок проведения совещаний (переговоров) по конфиденциальным вопросам.

Организацию совещаний (переговоров) по конфиденциальным вопросам можно разделить на три основных этапа:

- этап подготовки к проведению совещания (переговоров);
- этап непосредственного проведения совещания (переговоров);
- этап после проведения (оформление результатов) совещания (переговоров).

Для проведения совещания (переговоров) по конфиденциальным вопросам, прежде всего, необходимо получить разрешение, которое может давать руководитель организации или его заместитель (по курируемым вопросам), а в некоторых случаях — руководитель вышестоящей организации, в зависимости от ценности конфи-

циальной информации и состава участников, которых предполагается привлечь на совещание (переговоры).

В целях получения такого разрешения, и назначения лиц, ответственных за его подготовку, руководителем заинтересованного подразделения составляется докладная записка на имя соответствующего должностного лица, уполномоченного принимать решение.

В некоторых случаях, все эти вопросы определяет сам руководитель организации (предприятия) и назначает должностное лицо, которому поручается подготовка такого совещания (переговоров).

В докладную записку включаются:

- тематика совещания (переговоров) и основания для его проведения;
- перечень конфиденциальных вопросов (в том числе конфиденциальных изделий), которые планируются рассмотреть на совещании (переговорах);
- сроки проведения совещания (переговоров);
- место проведения совещания (переговоров);
- список сотрудников подразделений (организаций), участвующих в совещании (приглашенных на переговоры);
- список сотрудников подразделений, ответственных за подготовку и проведение совещания (переговоров).

Докладная записка подлежит согласованию с руководителями подразделений, участвующих в подготовке совещания (переговоров) и при необходимости может иметь гриф конфиденциальности.

В список сотрудников подразделений, ответственных за подготовку и проведение совещания (переговоров), как правило, включаются следующие лица:

- организатор совещания (переговоров) — должностное лицо, ответственное за подготовку и проведение совещания (переговоров) в целом, планирующее и координирующее выполнение всех подготовительных мероприятий и проведение самого совещания (переговоров); как правило, это руководитель заинтересованного подразделения (или должностное лицо, в чью сферу обязанностей входят рассматриваемые вопросы);

- должностное лицо, ответственное за защиту конфиденциальной информации при проведении совещания (переговоров); данный сотрудник несет ответственность за подготовку помещения, в котором будет проводиться мероприятие, осуществляет контроль защиты информации в ходе совещания (переговоров), пресекает несанкционированные действия участников совещания (переговоров), а также участвует в устранении последствий, вызванных данными действиями (как правило, это сотрудник службы безопасности);
- сотрудники, ответственные за подготовку материально-технического обеспечения (плакаты, образцы продукции, фото- и видеоаппаратура, проекторы, ноутбуки и т. п.), если эти лица привлекаются из разных подразделений.

При этом вопросы, связанные с функциональными обязанностями сотрудников специальных подразделений в докладной записке не указываются, они осуществляются на основании решения о проведении совещания (переговоров). Например, выдачу и учет носителей конфиденциальной информации (для ведения записей во время совещания) осуществляют сотрудники конфиденциального делопроизводства. Если обеспечение режима конфиденциальности при проведении таких мероприятий возложено должностными инструкциями (обязанностями) на службу безопасности, то ответственность за подготовку помещения, пропускной режим, выделение необходимого количества сотрудников охраны и осуществление других мер по защите информации несет начальник этого подразделения.

Одним из важнейших элементов при подготовке совещания (переговоров) является определение состава его участников.

В организацию, с которой предполагается проведение переговоров, направляется специальное письмо (приглашение), в котором содержится:

- тематика переговоров, обобщенный список предполагаемых участников;
- время и место проведения;
- предложение принять участие в переговорах или сообщить о своем отказе;

- предложение направить список сотрудников (представителей), которые будут участвовать в данном мероприятии (с указанием выступающих по конкретным вопросам), с подтверждением их доступа к конфиденциальной информации.

Такое приглашение (письмо), как правило, должно иметь гриф конфиденциальности по соответствующему виду тайны. В письме оговариваются и другие вопросы, связанные с конкретными переговорами и режимом их проведения.

Приглашение на совещания лиц, не являющихся сотрудниками организации (предприятия), разрешается только в случае крайней необходимости их личного участия в обсуждении конкретного вопроса (эксперты, консультанты). В этом случае они заранее предупреждаются об ответственности за разглашение конфиденциальной информации и дают письменное обязательство о неразглашении полученных сведений. Присутствие их при обсуждении других вопросов не разрешается.

Наличие доступа к конфиденциальной информации у сотрудников организации (предприятия), в которой проводится совещание (переговоры), проверяется службой безопасности организации (предприятия). Если в совещании (переговорах) необходимо участие сотрудника, не имеющего доступа к конфиденциальной информации, то ему оформляют доступ в соответствии с системой доступа, действующей в организации (на предприятии).

Наличие доступа у представителей приглашенной на совещание (переговоры) организации (предприятия) также проверяется службой безопасности, в соответствии со списком сотрудников, направленных для участия в данном мероприятии. Список должен быть оформлен в установленном порядке, иметь подпись руководителя и заверяться печатью организации (предприятия).

В процессе подготовки и согласования (уточнения) всех вопросов совещания (переговоров) составляются и по мере готовности утверждаются следующие документы:

- программа проведения совещания (переговоров). В данном документе указывается точная дата и время проведения мероприятия, повестка дня, в которой перечисляются вопросы, подлежащие обсуждению.

докладчики (выступающие), ориентировочное время работы (обсуждения каждого пункта повестки), а также информационные материалы, необходимые для детальной проработки поставленных вопросов. В случае если программа проведения совещания (переговоров) содержит конфиденциальную информацию, этот документ должен иметь гриф конфиденциальности;

- список участников совещания (переговоров) по каждому вопросу повестки дня. В списке участников указываются инициалы и фамилии лиц, занимаемые ими должности и представляемые организации (предприятия). Отдельно указываются наименования и номера документов, подтверждающих возможность их ознакомления с конфиденциальной информацией и полномочия принимать решения. Название представляемой организации может при необходимости заменяться ее условным обозначением;
- список материально-технического обеспечения (как конфиденциального, так и открытого) и ответственных за него лиц.

Планирование очередности решаемых вопросов должно осуществляться в зависимости:

- от ценности конфиденциальной информации (чем выше ценность информации, тем позднее вопрос ставится на повестку дня);
- от числа лиц, принимающих участие в обсуждении (чем меньше участников задействовано в обсуждении вопроса, тем позднее он ставится на повестку дня).

К участию в обсуждении вопроса привлекаются только те лица, которые имеют непосредственное отношение к этому вопросу. Это правило касается как сотрудников организации (предприятия), так и приглашенных лиц.

Любое совещание или переговоры по конфиденциальным вопросам проводятся только в специальном (выделенном) помещении, оборудованном средствами технической защиты информации. Целесообразно, чтобы помещение было аттестовано, а используемые в нем технические средства сертифицированы.

Помимо средств технической защиты информации помещение желательно оборудовать кондиционером, т. к. открытие окон и дверей в ходе совещания (переговоров) не допускается.

Перед проведением совещания (переговоров) необходимо:

- проверить помещение на наличие в нем несанкционированных аудио- и видеозаписывающих или радио-передающих устройств. В выделенном помещении не должны находиться приборы, оборудование и технические средства, которые непосредственно не используются для обеспечения совещания (переговоров), например, телефоны городской сети, компьютеры, множительная техника, телевизионные и радиоприемники и др. (при необходимости они размещаются в соседней, изолированной комнате);
- убедиться в качественной работе средств технической защиты информации (если они применяются);
- осуществить другие меры по подготовке помещения (включить кондиционер, установить пост охраны у дверей и т. д.). Убедиться в наличии и безопасности (прежде всего с точки зрения защиты информации) материально-технического обеспечения.

Если какие-либо демонстрируемые средства (плакаты, изделия и др.) необходимо заранее разместить в помещении, (из-за их больших размеров или для обеспечения непрерывности рассматриваемых вопросов), то принимаются меры по недопущению преждевременного или самовольного ознакомления с конфиденциальной информацией, которая в них содержится. В случае если между подготовкой помещения и проведением совещания (переговоров) есть существенный разрыв во времени, полностью подготовленное помещение подлежит опечатыванию и (или) сдаче под охрану.

Проведение совещания (переговоров) в неприспособленных и необорудованных соответствующим образом помещениях не разрешается. Проведение таких мероприятий в режимных помещениях или на режимных территориях допускается в исключительных случаях и должно быть отдельно оговорено (обосновано) в докладной записке при получении разрешения на проведения совещания (переговоров).

Проход участников совещания (переговоров) в выделенное помещение осуществляется при ведении за ними обязательного персонального контроля. Такой контроль, как правило, осуществляет назначенный сотрудник службы безопасности в соответствии с утвержденным списком и предъявляемыми персональными документами. Участникам совещания (переговоров) могут выдаваться специальные разовые пропуска (подготовленные заранее), а также организовываться их встреча и сопровождение. Все это повышает организованность и безопасность проведения мероприятия.

Перед началом обсуждения каждого нового вопроса состав присутствующих корректируется. Нахождение (ожидание) в помещении лиц, в том числе сотрудников данной организации (предприятия), не имеющих отношения к обсуждаемому вопросу, не разрешается.

Сотрудник (сотрудники) службы безопасности, осуществляя персональный контроль прохождения участников на совещание (переговоры), напоминает им о запрете проноса и использования фото-, кино-, видеоаппаратуры, ноутбуков, магнитофонов (в том числе плееров, радиоприемников, мобильных телефонов) и другой аппаратуры, кроме специально выделенной для этих целей (учтенной службой безопасности). Для этого необходимо предусмотреть место и порядок сдачи на временное хранение таких технических средств и возврата их владельцам после совещания (переговоров). В крайнем случае, допускается оставлять эти средства у участников, но с обязательным отключением аккумуляторов в мобильных телефонах, диктофонах и т. д.

Перед непосредственным началом совещания (переговоров) сотрудник, ответственный за проведение совещания (переговоров) или за защиту конфиденциальной информации при их проведении, должен предупредить участников о необходимости сохранения конфиденциальности информации, уточнив при этом, какие сведения к ней относятся.

Также целесообразно напомнить участникам, что им не следует:

- обсуждать вопросы, вынесенные на совещание (переговоры), вне выделенных помещений;
- информировать о совещании (переговорах), в вопросах повестки дня, составе участников, времени и месте проведения, ходе обсуждения вопросов,

содержании решений и т. п. любых лиц, не участвующих в данном совещании (переговорах), в том числе сотрудников своей организации (предприятия).

Участникам совещания (переговоров) при необходимости выдаются заранее подготовленные носители конфиденциальной информации для рабочих записей (блокноты, тетради и др.), при этом не допускается использование разрозненных листов. Все записи должны вестись только на данных носителях.

Конфиденциальные материалы и собственные носители информации участников совещания (переговоров) могут быть заранее направлены установленным порядком в организацию проводящую данное мероприятие. После их регистрации подразделением конфиденциального делопроизводства, они выдаются их владельцам — участникам совещания (переговоров).

По окончании совещания (переговоров) носители информации, выданные участникам для ведения записей, сдаются сотруднику подразделения конфиденциального делопроизводства и в дальнейшем направляются (или возвращаются) в организации (на предприятия) участников данного мероприятия. Невостребованные носители уничтожаются установленным порядком.

Аудио- и видеозапись, фотографирование конфиденциальных совещаний (переговоров) ведется только по письменному разрешению лица, давшего согласие на проведение совещания (переговоров) и осуществляется специально назначенным сотрудником организации (предприятия) на учтенных носителях.

Участники совещания (переговоров), замеченные в ведении несанкционированной аудио- или видеозаписи, использовании средств связи других неучтенных носителей, фотографировании, лишаются права дальнейшего присутствия на совещании (переговорах). По данному факту составляется акт, копия которого высылается руководителю организации (предприятия), направившего этого участника.

Одновременно носитель несанкционированно записанной информации изымается сотрудником службы безопасности для проведения внутреннего расследования и

уничтожения записанной информации. После этого носитель возвращается владельцу.

По окончании конфиденциального совещания (переговоров) помещение, в котором оно проходило, осматривается сотрудником службы безопасности. Обнаруженные в ходе проверки носители информации, выдававшиеся участникам для ведения записей, передаются в подразделение конфиденциального делопроизводства. При обнаружении неучтенных носителей или несанкционированных технических средств, об этом докладывается руководителю организации (предприятия) и принимаются меры для предотвращения возможных негативных последствий.

Специально назначенный сотрудник ведет протокол совещания (переговоров), который в дальнейшем (после оформления) утверждается руководителем организации (предприятия) и имеет соответствующий гриф конфиденциальности.

Утвержденный протокол, с материалами совещания (переговоров), а также результаты проверочных мероприятий по его завершении, подлежат учету и хранению в подразделении конфиденциального делопроизводства.

Документы, принятые на совещании (переговорах), оформляются, подписываются и учитываются в соответствии с требованиями по работе с конфиденциальными документами организации (предприятия). Все экземпляры этих документов должны иметь соответствующий гриф конфиденциальности. Направление этих документов организациям (предприятиям) принявшим участие в совещании (переговорах) осуществляется порядком, установленным для конфиденциальных документов.

На имя руководителя, давшего разрешение на проведение совещания (переговоров), пишется докладная записка о ходе и результатах проведения совещания (если это лицо не принимало личного участия в данном мероприятии), с соблюдением режима конфиденциальности. К докладной записке прикладываются необходимые документы.

При проведении переговоров с незнакомой по совместной работе организацией (предприятием) следует достаточно осторожно относиться к ознакомлению их представителей со сведениями, составляющими коммерческую или служебную тайну. Иногда переговоры прово-

дятся именно с целью получения конфиденциальной информации под предлогом дальнейшего сотрудничества, а не с целью заключения контракта.

В любом случае сотрудникам организации (предприятия), организующим переговоры, не разрешается использовать в дискуссии конфиденциальную информацию, не относящуюся к обсуждаемому вопросу, раскрывать желаемые результаты переговоров, а также итоги аналогичных переговоров с другими партнерами. Состав оглашаемых конфиденциальных сведений регламентируется руководителем, организовавшим совещание, и доводится до всех участников, которые готовят (проводят) это мероприятие.

В случае имевших место нарушений режима коммерческой (служебной) тайны при проведении совещания (переговоров), выявления фактов (утроз) утраты конфиденциальных документов или разглашения содержащейся в них информации, назначается внутреннее расследование и принимаются меры по предотвращению возможных негативных последствий.

ПРОВЕДЕНИЕ ВНУТРЕННИХ РАССЛЕДОВАНИЙ ПО ФАКТАМ УТРАТЫ (РАЗГЛАШЕНИЯ) КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

По фактам утраты (в том числе временной) конфиденциальных документов (носителей, изделий), разглашения охраняемой законом информации, а также другим нарушением режима коммерческой или служебной тайны проводятся внутренние расследования.

Расследования имеют целью:

- поиск утраченного документа (носителя, изделия);
- изучение (анализ) ситуации для принятия мер по предотвращению (пресечению) повторения выявленного нарушения;
- создание доказательной базы для привлечения виновных лиц к установленной законодательством ответственности.

Факт выявления нарушения режима коммерческой (служебной) тайны должен быть зафиксирован документально — в виде служебной записки, заявления, рапорта, акта и т. п. На основании этого документа назначается внутреннее расследование. Если факт нарушения не зафиксирован, но есть предположение о его совершении (или сокрытии факта нарушения) назначается соответствующая внутренняя проверка. Результаты проверки также могут стать основанием для проведения расследования.

Задачами внутреннего расследования являются:

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
- обследование мест возможного нахождения утраченного конфиденциального документа (носителя, изделия и т. п.);

- установление лиц, непосредственно виновных в данном нарушении;
- выявление причин и условий, способствовавших нарушению.

Для проведения внутреннего расследования руководитель организации (предприятия) приказом или распоряжением назначает комиссию в составе не менее трех человек. Комиссия должна быть сформирована не позднее следующего дня после даты выявления нарушения из компетентных и не заинтересованных в исходе разбирательства сотрудников. Они должны быть допущены к коммерческой (служебной) тайне и иметь отношение к рассматриваемому вопросу. В состав комиссии целесообразно включать представителя службы безопасности и конфиденциального делопроизводства, представителя подразделения, в котором зафиксировано нарушение (но не состоящего в подчиненности с лицами, в отношении которых проводится расследование), юриста (сотрудника кадрового подразделения).

Если имеется вышестоящая организация, то о факте выявленного нарушения и назначении внутреннего расследования информируется руководитель подразделения (должностное лицо), отвечающее за защиту информации в этой организации. Вышестоящая организация может направить своего представителя для участия в работе комиссии, возглавить ее или назначить свою комиссию.

На время проведения мероприятий по расследованию члены комиссии освобождаются от исполнения своих должностных обязанностей. Общая продолжительность внутреннего расследования не должна превышать одного месяца.

Комиссия обязана принять исчерпывающие меры для всестороннего и объективного изучения и документального оформления всех обстоятельств нарушения.

Для того чтобы выполнить поставленные задачи, комиссия должна быть наделена определенными полномочиями, которые целесообразно закрепить в соответствующем разделе «Положения о режиме коммерческой (служебной) тайны организации (предприятия)» или самостоятельном документе (инструкции).

В общем виде права и обязанности комиссии включают в себя:

- опрос работников, допустивших утрату документов (носителей, изделий) или разглашение конфиденциальной информации, а также лиц, которые могут оказать содействие в установлении обстоятельств произошедшего;
- проведение осмотров территории, здания, помещений (комнат, кабинетов), хранилищ, сейфов, шкафов, спецпюльфов, столов и других объектов и предметов, которые могут иметь отношение к факту нарушения или в которых могут находиться утраченные документы;
- проверку всех конфиденциальных документов, а также журналов (карточек) учета и сопроводительных документов, отражающих поступление и движение утраченных документов;
- привлечение (с разрешения соответствующего руководителя) других работников к проведению отдельных действий в рамках внутреннего расследования.

Работник, в отношении которого проводится расследование, должен быть ознакомлен с приказом (распоряжением) о проведении расследования.

Все действия членов комиссии и полученные в ходе расследования материалы подлежат письменному оформлению (актами, справками и т. п.).

Истребование от работника объяснения в письменной форме для установления причины нарушения является обязательным. В случае, когда работник отказывается дать письменные объяснения, его устные показания или отказ от них письменно фиксируются членами комиссии (не менее чем за двумя подписями).

В целях исключения возможности какого-либо воздействия на процесс расследования члены комиссии обязаны соблюдать конфиденциальность расследования до принятия по ним решения руководителем организации (предприятия).

Для организованного и оперативного проведения внутреннего расследования комиссия разрабатывает версии причин нарушения (например, о возможном местонахождении пропавшего документа) и составляет план про-

ведения необходимых мероприятий (поиска) по каждой из этих версий. В ходе расследования могут выдвигаться и обрабатываться дополнительные версии (с соответствующим уточнением плана действий).

После того как возможные меры поиска документа (носителя, изделия) исчерпаны, но не привели к его обнаружению, полностью выяснены обстоятельства утраты и установлены виновные лица, поиск документа может быть прекращен. Решение о прекращении поиска утверждает должностным лицом, назначившим внутреннее расследование (по мотивированному заключению комиссии).

Одновременно с комиссией по проведению внутреннего расследования руководитель организации (предприятия) может поручить экспертной комиссии организации (предприятия) определить актуальность утраченной (разглашенной) конфиденциальной информации, а также назначить комиссию по определению (подсчету) ущерба (убытков) по расследуемому факту, из компетентных и незаинтересованных должностных лиц. Указанные задачи могут возлагаться на одну комиссию (с назначением в ее состав соответствующих специалистов).

Сумма ущерба либо убытков и методика ее расчета должны быть обоснованы и утверждены. В отдельных случаях такая оценка может быть осуществлена специализированной организацией.

Актуальность конфиденциальных сведений, поступивших из другой организации (предприятия), и размер ущерба от их разглашения (утраты) определяются этой организацией.

Заключения экспертной комиссии и комиссии по определению ущерба (убытков) должны быть подготовлены до окончания проведения внутреннего расследования. Это необходимо для того, чтобы принять исчерпывающие меры по локализации последствий данного нарушения и объективно определить меру ответственности виновных лиц.

По окончании внутреннего расследования комиссия представляет руководителю организации (предприятия) заключение, в котором излагаются:

- основания и время проведения расследования;
- проделанная работа (кратко);

- время, место и обстоятельства факта нарушения;
- причины и условия совершения нарушения;
- виновные лица и степень их вины;
- наличие умысла в действиях виновных лиц;
- предложения по возмещению ущерба;
- предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия;
- рекомендации по исключению подобных нарушений;
- предложения по прекращению поиска конфиденциального документа (носителя, изделия) и списанию его с учетных форм;
- другие вопросы, поставленные перед комиссией (об актуальности конфиденциальной информации, о размерах ущерба и т. д.).

В случае нахождения во время расследования утерянного документа (носителя, изделия) в заключении комиссии отражаются причины его временного отсутствия.

К заключению прилагаются:

- письменные объяснения лиц, которых опрашивали члены комиссии;
- акты (справки) проверок конфиденциальных документов (носителей, изделий), осмотров помещений, хранилищ и т. д.;
- другие документы (копии документов), относящиеся к расследованию, в том числе заключения экспертной комиссии и комиссии по определению размеров ущерба (убытков).

Заключение должно быть подписано всеми членами комиссии. При несогласии с выводами или содержанием отдельных положений член комиссии, подписывая заключение, приобщает к нему свое особое мнение (в письменном виде).

Заключение по результатам расследования подлежит утверждению должностным лицом, назначившим это расследование.

Работник, в отношении которого проводится расследование, или его уполномоченный представитель имеют право знакомиться с материалами расследования и требо-

вать приобщения к материалам расследования представляемых ими документов и материалов.

Работник, в отношении которого проведено расследование, должен быть ознакомлен с его результатами, что удостоверяется его подписью на утвержденном заключении.

Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется приказом.

При наличии в действиях лица признаков административного правонарушения или уголовного преступления руководитель организации (предприятия) обязан обращаться в правоохранительные органы для привлечения виновного к ответственности в соответствии с законодательством.

В соответствии с Трудовым кодексом возмещение ущерба производится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

При несогласии работника с результатами подсчета ущерба взыскание должно производиться по решению суда. В этом случае заключение по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нарушение режима конфиденциальности.

Первый экземпляр, заключения, с резолюцией утвердившего его руководителя, копия приказа (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, и копию приказа (распоряжения) о назначении комиссии (комиссий), подлежат хранению в отдельном деле.

При необходимости заключение и материалы расследования могут иметь гриф конфиденциальности. В этом случае они учитываются по журналу учета изданных документов и хранятся в подразделении конфиденциального делопроизводства.

Один экземпляр заключения направляется в вышестоящую организацию (если она есть).

На основании утвержденного заключения комиссии (приказа) сотрудники конфиденциального производства

осуществляют списание утраченного документа (носителя, изделия) с учета: в соответствующих учетных формах ставятся отметки о списании (со ссылкой на номер и дату утвержденного заключения или приказа). При необходимости составляется акт о списании.

Учет утрат конфиденциальных документов (носителей, изделий) или фактов разглашения информации, составляющей коммерческую (служебную) тайну, ведется в специальном журнале учета (см. гл. XIII). Анализ материалов расследования позволяет разработать конкретные меры по предотвращению нарушений режима охраняемой законом тайны.

Весь текст остальной страницы и нижних страниц книги является очень размытым и нечитаемым из-за плохого качества сканирования. Видно лишь призрачные очертания абзацев и строчек, но содержание невозможно извлечь.

Глава XVII

ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

В настоящее время все большее количество информационных ресурсов сосредотачивается на электронных носителях.

В традиционном документообороте средства ЭВМ выполняют лишь вспомогательную функцию — подготовку проекта документа. В этом случае электронная форма документа является не более чем технологическим эпизодом, в интервале от формирования документа на ЭВМ до распечатки на принтере. Эта работа осуществляется на защищенных СВТ и в защищенных помещениях и не требует изменения принципов организации конфиденциального делопроизводства.

Полномасштабное применение ЭВМ при обработке информации, перенос документооборота с бумажных носителей в электронную среду является новым этапом развития процессов управленческой, научно-технической и коммерческой деятельности, позволяющим значительно повысить оперативность и «прозрачность» обращения документов.

Для все большего числа документов электронная форма становится постоянной или почти постоянной, что существенно усложняет проблему защиты информации, требует организации делопроизводства на иных, по сравнению с прежним документооборотом, принципах.

В общем виде электронный документ представляет собой цифровое отображение информации, носителем которого являются средства вычислительной техники и информатики. Электронный документ непосредственно воспринимается только объектами электронной среды — техническими и программными средствами.

Современные системы электронного документооборота успешно решают задачи автоматизации делопроизводства. При этом они включают в себя не просто приложения, предназначенные для перевода бумажных документов в электронный вид, а являются полноценным инструментом управления.

Системы электронного документооборота организуют все процессы жизненного цикла документа, включая работу над проектами, согласование, утверждение (подписание), исполнение, отправку в «дело» или архив.

Кроме того, эти системы обеспечивают необходимый сервис для хранения, поиска и систематизации электронных документов, а также разделения прав доступа к ним.

Рост числа внедренных систем электронного документооборота наблюдается как в коммерческих, так и в государственных организациях. Применяемые системы электронного документооборота достаточно разнообразны и построены на различных подходах. Основным достоинством отечественных систем является учет российских традиций делопроизводства, заложенный в логику их работы.

Развитие электронного документооборота изначально строилось на соблюдении требования защиты информации — сохранении от искажений, утрат и в определенной мере от ознакомления с нею посторонних лиц.

В качестве угроз безопасности электронной информации выступают: внутренние составляющие (персонал организации предприятия); внешние (хакеры, «компьютерные вирусы»), а также особенности среды передачи данных (возможное искажение либо перехват информации при использовании открытых каналов связи, в том числе через Интернет) и, кроме того, возможные сбои оборудования (программ).

Эти угрозы достаточно серьезны и, несмотря на высокие показатели надежности существующих систем электронного документооборота, уровень развития аппаратного и программного обеспечения не гарантирует абсолютной надежности хранения и передачи информации в электронном виде.

Другой недостаток таких систем — необходимость специальных знаний и навыков для работы с соответствующим программным и аппаратным обеспечением, а также организации контроля этой работы.

Для решения проблем надежной защиты информации в системах электронного документооборота используется целый ряд программно-аппаратных систем и средств, таких как:

- системы защиты информации от несанкционированного доступа;
- системы защиты от атак из внешних сетей, в том числе через Интернет;
- средства криптографической защиты информации — электронная цифровая подпись и шифрование (с использованием алгоритмов с симметричным и несимметричными ключами);
- средства защиты от «компьютерных вирусов» и другие.

Эти системы и средства разрабатываются специализированными компаниями, продукция которых сертифицируется соответствующими государственными органами, и в готовом виде встраиваются в системы электронного документооборота. Кроме того, все информационные системы государственных организаций подлежат обязательной сертификации.

При обработке в электронных системах конфиденциальных документов требования к защите информации многократно возрастают. Надежная защита информации в системах электронного документооборота достигается комплексным применением как программно-аппаратных систем и средств, так и реализацией организационных (в том числе режимных) мероприятий.

В общем виде системы электронного документооборота, в которых циркулирует конфиденциальная информация, должны обеспечивать:

- идентификацию (аутентификацию) каждого пользователя;
- невозможность отказа от созданного исполнителем документа или действий над ним — за счет закрепления за каждым сотрудником электронной цифровой подписи;
- полноту и целостность информации (документа) — за счет автоматической проверки электронной цифровой подписи;
- шифрование конфиденциальной информации при ее передаче;

- шифрование базы данных на жестком диске сервера;
- импорт идентификационных данных — исключая возможность обмена информацией с «подставным» сервером;
- защиту от сбоев;
- наличие программируемых (гибких) грифов доступа (в том числе по правам копирования, печати и отправке документов) и другие.

Но даже в этом случае остаются проблемные вопросы безопасности информации, например: возможность доступа администратора сети к любой информации; риск хищения идентификационных (аутентификационных) данных; несанкционированное копирование информации и ряд других.

В качестве противодействия таким угрозам применяются рассмотренные в предыдущих главах меры: определение перечня (состава) конфиденциальной информации (документов); организация жесткой системы доступа — оптимизация круга сотрудников допускаемых к разным уровням информации; регулярная проверка сотрудников службой безопасности; обучение персонала; установление четко регламентированного порядка электронного документирования, позволяющего контролировать прохождение, хранение, копирование и уничтожение документов.

Организация доступа к конфиденциальным массивам электронных документов, базам данных подразумевает: определение и регламентацию состава сотрудников, допускаемых к работе с определенными файлами; контроль доступа администратором базы данных; фиксирование в машинной памяти имен пользователей и операторов, имеющих право доступа; учет состава базы данных и файлов, регулярную проверку наличия, целостности и комплектности электронных документов; регистрацию входа в базу данных; автоматическую регистрацию имен пользователей и времени работы; регистрацию попыток несанкционированного входа в систему; регистрацию ошибочных (неразрешенных) действий пользователя; автоматическое блокирование доступа и подачу сигнала тревоги и др.

Вся информация должна гарантированно иметь страховые копии с отдельной системой доступа (исключающей возможность их изменения).

В некоторых случаях целесообразно также организовать копирование, печать и отправку документов через отдельные процедуры.

Все эти вопросы должны быть строго регламентированы в Положении о коммерческой (служебной) тайне организации (предприятия) или самостоятельном документе.

В любом случае, выбирая систему электронного документооборота и дополняя ее программными и аппаратными средствами для обращения конфиденциальных документов необходимо четко представлять возможность этой системы с точки зрения защиты от угроз (рисков) безопасности информации и не пренебрегать традиционными мерами режима и контроля.

■ ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1

ФЕДЕРАЛЬНЫЙ ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:
 - 1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
 - 2) применении информационных технологий;
 - 3) обеспечении защиты информации.
2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

В настоящем Федеральном законе используются следующие основные понятия:

- 1) информация — сведения (сообщения, данные) независимо от формы их представления;
- 2) информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- 3) информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

- 4) информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
- 5) обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- 6) доступ к информации — возможность получения информации и ее использования;
- 7) конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- 8) предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
- 9) распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
- 10) электронное сообщение — информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
- 11) документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
- 12) оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

- 1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- 2) установление ограничений доступа к информации только федеральными законами;
- 3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- 4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- 5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- 6) достоверность информации и своевременность ее предоставления;
- 7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- 8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Статья 4. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации

1. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Фе-

дерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

2. Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.
3. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

Статья 5. Информация как объект правовых отношений

1. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.
2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).
3. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:
 - 1) информацию, свободно распространяемую;
 - 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
 - 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
 - 4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.
4. Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Статья 6. Владелец информации

1. Владелелем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.
2. От имени Российской Федерации, субъекта Российской Федерации, муниципального образования полномочия владельца информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.
3. Владелелем информации, если иное не предусмотрено федеральными законами, вправе:
 - 1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
 - 2) использовать информацию, в том числе распространять ее, по своему усмотрению;
 - 3) передавать информацию другим лицам по договору или на ином установленном законом основании;
 - 4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
 - 5) осуществлять иные действия с информацией или разрешать осуществление таких действий.
4. Владелец информации при осуществлении своих прав обязан:
 - 1) соблюдать права и законные интересы иных лиц;
 - 2) принимать меры по защите информации;
 - 3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Статья 7. Общедоступная информация

1. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.
2. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

3. Владелец информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Статья 8. Право на доступ к информации

1. Граждане (физические лица) и организации (юридические лица) (далее — организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.
2. Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.
3. Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.
4. Не может быть ограничен доступ к:
 - 1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
 - 2) информации о состоянии окружающей среды;
 - 3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
 - 4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

- 5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.
5. Государственные органы и органы местного самоуправления обязаны обеспечивать доступ к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.
6. Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.
7. В случае, если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.
8. Предоставляется бесплатно информация:
- 1) о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;
 - 2) затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;
 - 3) иная установленная законом информация.
9. Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

Статья 9. Ограничение доступа к информации

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.
2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.
3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.
4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.
5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.
6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.
7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.
8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.
9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

Статья 10. Распространение информации или предоставление информации

1. В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.
2. Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица.
3. При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации.
4. Предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.
5. Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.
6. Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Статья 11. Документирование информации

1. Законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.
2. В федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством Российской Федерации. Правила делопроизводства и документооборота, установленные иными государственными органами, органами местного самоуправления в пределах их ком-

петенции, должны соответствовать требованиям, установленным Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти.

3. Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.
4. В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.
5. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

Статья 12. Государственное регулирование в сфере применения информационных технологий

1. Государственное регулирование в сфере применения информационных технологий предусматривает:
 - 1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;
 - 2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и ор-

- ганов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;
- 3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети Интернет и иных подобных информационно-телекоммуникационных сетей.
2. Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:
- 1) участвуют в разработке и реализации целевых программ применения информационных технологий;
 - 2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Статья 13. Информационные системы

1. Информационные системы включают в себя:
 - 1) государственные информационные системы — федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;
 - 2) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;
 - 3) иные информационные системы.
2. Если иное не установлено федеральными законами, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.
3. Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных.

4. Установленные настоящим Федеральным законом требования к государственным информационным системам распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении.
5. Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем.
6. Порядок создания и эксплуатации информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, определяется операторами таких информационных систем в соответствии с требованиями, установленными настоящим Федеральным законом или другими федеральными законами.

Статья 14. Государственные информационные системы

1. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.
2. Государственные информационные системы создаются с учетом требований, предусмотренных Федеральным законом от 21 июля 2005 года № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».
3. Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

4. Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления — Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами.
5. Если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы. При этом ввод государственной информационной системы в эксплуатацию осуществляется в порядке, установленном указанным заказчиком.
6. Правительство Российской Федерации вправе устанавливать обязательные требования к порядку ввода в эксплуатацию отдельных государственных информационных систем.
7. Не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности.
8. Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.
9. Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами.

Статья 15. Использование информационно-телекоммуникационных сетей

1. На территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи, настоящего Федерального закона и иных нормативных правовых актов Российской Федерации.

2. Регулирование использования информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, осуществляется в Российской Федерации с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области. Порядок использования иных информационно-телекоммуникационных сетей определяется владельцами таких сетей с учетом требований, установленных настоящим Федеральным законом.
3. Использование на территории Российской Федерации информационно-телекоммуникационных сетей в хозяйственной или иной деятельности не может служить основанием для установления дополнительных требований или ограничений, касающихся регулирования указанной деятельности, осуществляемой без использования таких сетей, а также для несоблюдения требований, установленных федеральными законами.
4. Федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть при осуществлении предпринимательской деятельности. При этом получатель электронного сообщения, находящийся на территории Российской Федерации, вправе провести проверку, позволяющую установить отправителя электронного сообщения, а в установленных федеральными законами или соглашением сторон случаях обязан провести такую проверку.
5. Передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть ограничена только в порядке и на условиях, которые установлены федеральными законами.
6. Особенности подключения государственных информационных систем к информационно-телекоммуникационным сетям могут быть установлены нормативным правовым актом Президента Российской Федерации или нормативным правовым актом Правительства Российской Федерации.

Статья 16. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:
 - 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
 - 2) соблюдение конфиденциальности информации ограниченного доступа;
 - 3) реализацию права на доступ к информации.
2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.
3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.
4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:
 - 1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
 - 2) своевременное обнаружение фактов несанкционированного доступа к информации;
 - 3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
 - 4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
 - 5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
 - 6) постоянный контроль за обеспечением уровня защищенности информации.

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.
6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

1. Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.
2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.
3. В случае, если распространение определенной информации ограничивается или запрещается федеральными

ми законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

- 1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;
- 2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

Статья 18. О признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации

Со дня вступления в силу настоящего Федерального закона признать утратившими силу:

- 1) Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» (Собрание законодательства Российской Федерации, 1995, № 8, ст. 609);
- 2) Федеральный закон от 4 июля 1996 года № 85-ФЗ «Об участии в международном информационном обмене» (Собрание законодательства Российской Федерации, 1996, № 28, ст. 3347);
- 3) статью 16 Федерального закона от 10 января 2003 года № 15-ФЗ «О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона «О лицензировании отдельных видов деятельности» (Собрание законодательства Российской Федерации, 2003, № 2, ст. 167);
- 4) статью 21 Федерального закона от 30 июня 2003 года № 86-ФЗ «О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации, признании утратившими силу отдельных законодательных актов Российской Федерации, предоставлении отдельных гарантий сотрудникам органов внутренних дел, органов по контролю за оборотом наркотических средств и психотропных веществ и упраздняемых федеральных органов налоговой полиции в связи с осуществлением мер по совершенствованию государственного управле-

ния» (Собрание законодательства Российской Федерации, 2003, № 27, ст. 2700);

- 5) статью 39 Федерального закона от 29 июня 2004 года № 58-ФЗ «О внесении изменений в некоторые законодательные акты Российской Федерации и признании утратившими силу некоторых законодательных актов Российской Федерации в связи с осуществлением мер по совершенствованию государственного управления» (Собрание законодательства Российской Федерации, 2004, № 27, ст. 2711).

Президент Российской Федерации

Москва, Кремль

27 июля 2006 года

№ 149-ФЗ

ПРИЛОЖЕНИЕ 2

ФЕДЕРАЛЬНЫЙ ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ О КОММЕРЧЕСКОЙ ТАЙНЕ

(в редакции Федерального закона от 02.02.2006 № 19-ФЗ)

Статья 1. Цели и сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну.
2. Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.
3. Положения настоящего Федерального закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

**Статья 2. Законодательство Российской Федерации
о коммерческой тайне**

Законодательство Российской Федерации о коммерческой тайне состоит из Гражданского кодекса Российской Федерации, настоящего Федерального закона, других федеральных законов.

**Статья 3. Основные понятия, используемые
в настоящем Федеральном законе**

Для целей настоящего Федерального закона используются следующие основные понятия:

- 1) коммерческая тайна — конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;
- 2) информация, составляющая коммерческую тайну, — научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства [ноу-хау]), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны;
- 3) режим коммерческой тайны — правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности;
- 4) обладатель информации, составляющей коммерческую тайну, — лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;
- 5) доступ к информации, составляющей коммерческую тайну, — ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

- 6) передача информации, составляющей коммерческую тайну, — передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;
- 7) контрагент — сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;
- 8) предоставление информации, составляющей коммерческую тайну, — передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;
- 9) разглашение информации, составляющей коммерческую тайну, — действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Статья 4. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации

1. Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона.
2. Информация, самостоятельно полученная лицом при осуществлении исследований, систематических наблюдений или иной деятельности, считается полученной законным способом несмотря на то, что содержание указанной информации может совпадать с содержанием информации, составляющей коммерческую тайну, обладателем которой является другое лицо.

3. Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.
4. Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

Статья 5. Сведения, которые не могут составлять коммерческую тайну

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

- 1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
- 2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- 3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
- 4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

- 5) требовать от юридических и физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;
- 6) требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, осуществленных случайно или по ошибке, охраны конфиденциальности этой информации;
- 7) защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

Статья 8. Владелец информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений

1. Владелелем информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений, является работодатель.
2. В случае получения работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя результата, способного к правовой охране в качестве изобретения, полезной модели, промышленного образца, топологии интегральной микросхемы, программы для электронных вычислительных машин или базы данных, отношения между работником и работодателем регулируются в соответствии с законодательством Российской Федерации об интеллектуальной собственности.

Статья 9. Порядок установления режима коммерческой тайны при выполнении государственного или муниципального контракта для государственных или муниципальных нужд

Государственным или муниципальным контрактом на выполнение научно-исследовательских, опытно-конструкторских, технологических или иных работ для го-

сударственных или муниципальных нужд должен быть определен объем сведений, признаваемых конфиденциальными, а также должны быть урегулированы вопросы, касающиеся установления в отношении полученной информации режима коммерческой тайны.

Статья 10. Охрана конфиденциальности информации

1. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:
 - 1) определение перечня информации, составляющей коммерческую тайну;
 - 2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
 - 3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
 - 4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
 - 5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц — полное наименование и место нахождения, для индивидуальных предпринимателей — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).
2. Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в части 1 настоящей статьи.
3. Индивидуальный предприниматель, являющийся обладателем информации, составляющей коммерческую тайну, и не имеющий работников, с которыми заключены трудовые договоры, принимает меры по охране конфиденциальности информации, указанные в части

- 1 настоящей статьи, за исключением пунктов 1 и 2, а также положений пункта 4, касающихся регулирования трудовых отношений.
4. Наряду с мерами, указанными в части 1 настоящей статьи, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.
5. Меры по охране конфиденциальности информации признаются разумно достаточными, если:
- 1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;
 - 2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.
6. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Статья 11. Охрана конфиденциальности информации в рамках трудовых отношений

1. В целях охраны конфиденциальности информации работодатель обязан:
- 1) ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты;
 - 2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;
 - 3) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

2. Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.
3. В целях охраны конфиденциальности информации работник обязан:
 - 1) выполнять установленный работодателем режим коммерческой тайны;
 - 2) не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях;
 - 3) не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, после прекращения трудового договора в течение срока, предусмотренного соглашением между работником и работодателем, заключенным в период срока действия трудового договора, или в течение трех лет после прекращения трудового договора, если указанное соглашение не заключалось;
 - 4) возместить причиненный работодателю ущерб, если работник виновен в разглашении информации, составляющей коммерческую тайну, ставшей ему известной в связи с исполнением им трудовых обязанностей;
 - 5) передать работодателю при прекращении или расторжении трудового договора имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую коммерческую тайну.
4. Работодатель вправе потребовать возмещения причиненных убытков лицом, прекратившим с ним трудовые отношения, в случае, если это лицо виновно в разглашении информации, составляющей коммерческую тайну, доступ к которой это лицо получило в связи с исполнением им трудовых обязанностей, если разглашение такой информации последовало в течение срока, установленного в соответствии с пунктом 3 части 3 настоящей статьи.
5. Причиненные ущерб либо убытки не возмещаются работником или прекратившим трудовые отношения лицом, если разглашение информации, составляющей

коммерческую тайну, явилось следствием непреодолимой силы, крайней необходимости или неисполнении работодателем обязанности по обеспечению режима коммерческой тайны.

6. Трудовым договором с руководителем организации должны предусматриваться его обязательства по обеспечению охраны конфиденциальности информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны ее конфиденциальности.
7. Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства Российской Федерации о коммерческой тайне. При этом убытки определяются в соответствии с гражданским законодательством.
8. Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением им трудовых обязанностей.

Статья 12. Охрана конфиденциальности информации в рамках гражданско-правовых отношений

1. Отношения между обладателем информации, составляющей коммерческую тайну, и его контрагентом в части, касающейся охраны конфиденциальности информации, регулируются законом и договором.
2. В договоре должны быть определены условия охраны конфиденциальности информации, в том числе в случае реорганизации или ликвидации одной из сторон договора в соответствии с гражданским законодательством, а также обязанность контрагента по возмещению убытков при разглашении им этой информации вопреки договору.
3. В случае, если иное не установлено договором между обладателем информации, составляющей коммерческую тайну, и контрагентом, контрагент в соответствии с законодательством Российской Федерации самостоятельно определяет способы защиты информации, составляющей коммерческую тайну, переданной ему по договору.

4. Контрагент обязан незамедлительно сообщить владельцу информации, составляющей коммерческую тайну, о допущенном контрагентом либо ставшем ему известным факте разглашения или угрозы разглашения, незаконном получении или незаконном использовании информации, составляющей коммерческую тайну, третьими лицами.
5. Владелец информации, составляющей коммерческую тайну, переданной им контрагенту, до окончания срока действия договора не может разглашать информацию, составляющую коммерческую тайну, а также в одностороннем порядке прекращать охрану ее конфиденциальности, если иное не установлено договором.
6. Сторона, не обеспечившая в соответствии с условиями договора охраны конфиденциальности информации, переданной по договору, обязана возместить другой стороне убытки, если иное не предусмотрено договором.

Статья 13. Охрана конфиденциальности информации при ее предоставлении

1. Органы государственной власти, иные государственные органы, органы местного самоуправления в соответствии с настоящим Федеральным законом и иными федеральными законами обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями.
2. Должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, государственные или муниципальные служащие указанных органов без согласия владельца информации, составляющей коммерческую тайну, не вправе разглашать или передавать другим лицам, органам государственной власти, иным государственным органам, органам местного самоуправления ставшую известной им в силу выполнения должностных (служебных) обязанностей информацию, составляющую коммерческую тайну, за исключением случаев, предусмотренных настоящим Федеральным законом, а также не вправе использовать эту информацию в корыстных или иных личных целях.
3. В случае нарушения конфиденциальности информации должностными лицами органов государственной власти,

иных государственных органов, органов местного самоуправления, государственными и муниципальными служащими указанных органов эти лица несут ответственность в соответствии с законодательством Российской Федерации.

Статья 14. Ответственность за нарушение настоящего Федерального закона

1. Нарушение настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.
2. Работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.
3. Органы государственной власти, иные государственные органы, органы местного самоуправления, получившие доступ к информации, составляющей коммерческую тайну, несут перед обладателем информации, составляющей коммерческую тайну, гражданско-правовую ответственность за разглашение или незаконное использование этой информации их должностными лицами, государственными или муниципальными служащими указанных органов, которым она стала известна в связи с выполнением ими должностных (служебных) обязанностей.
4. Лицо, которое использовало информацию, составляющую коммерческую тайну, и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайности или ошибки, не может в соответствии с настоящим Федеральным законом быть привлечено к ответственности.
5. По требованию обладателя информации, составляющей коммерческую тайну, лицо, указанное в части 4 настоящей статьи, обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять указанные меры обладатель информации, составляющей коммерческую тайну, вправе требовать в судебном порядке защиты своих прав.

Статья 15. Ответственность за непредоставление органам государственной власти, иным государственным органам, органам местного самоуправления информации, составляющей коммерческую тайну

Невыполнение обладателем информации, составляющей коммерческую тайну, законных требований органов государственной власти, иных государственных органов, органов местного самоуправления о предоставлении им информации, составляющей коммерческую тайну, а равно воспрепятствование получению должностными лицами этих органов указанной информации влечет за собой ответственность в соответствии с законодательством Российской Федерации.

Статья 16. Переходные положения

Гриффы, нанесенные до вступления в силу настоящего Федерального закона на материальные носители и указывающие на содержание в них информации, составляющей коммерческую тайну, сохраняют свое действие при условии, если меры по охране конфиденциальности указанной информации будут приведены в соответствие с требованиями настоящего Федерального закона.

*Президент Российской Федерации
Москва, Кремль. 29 июля 2004 года
№ 98-ФЗ*

ПРИЛОЖЕНИЕ 3

УТВЕРЖДЕНО
постановлением Правительства
Российской Федерации
от 3 ноября 1994 г. № 1233

ПОЛОЖЕНИЕ¹

**О ПОРЯДКЕ ОБРАЩЕНИЯ СО СЛУЖЕБНОЙ
ИНФОРМАЦИЕЙ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ
В ФЕДЕРАЛЬНЫХ ОРГАНАХ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ**

1. Общие положения

1.1. Настоящее Положение определяет общий порядок обращения с документами и другими материальными носителями информации (далее — документами), содер-

¹ Собрание законодательства Российской Федерации, 2005 г., выпуск 30 (часть II), ст. 3165.

жащими служебную информацию ограниченного распространения, в федеральных органах исполнительной власти, а также на подведомственных им предприятиях, в учреждениях и организациях (далее — организациях).

Положение не распространяется на порядок обращения с документами, содержащими сведения, составляющие государственную тайну.

1.2. К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью.

1.3. Не могут быть отнесены к служебной информации ограниченного распространения:

- акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
- сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;
- описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;
- порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;
- решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;
- сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;
- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

1.4. На документах (в необходимых случаях и на их проектах), содержащих служебную информацию огра-

ниченного распространения, проставляется пометка «Для служебного пользования».

1.5. Руководитель федерального органа исполнительной власти в пределах своей компетенции определяет:

- категории должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения;
- порядок передачи служебной информации ограниченного распространения другим органам и организациям;
- порядок снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения;
- организацию защиты служебной информации ограниченного распространения.

1.6. Должностные лица, принявшие решение об отнесении служебной информации к разряду ограниченного распространения, несут персональную ответственность за обоснованность принятого решения и за соблюдение ограничений, предусмотренных пунктом 1.3 настоящего Положения.

1.7. Служебная информация ограниченного распространения без санкции соответствующего должностного лица не подлежит разглашению (распространению).

1.8. За разглашение служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими такую информацию, государственный служащий (работник организации) может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

1.9. В случае ликвидации федерального органа исполнительной власти (организации) решение о дальнейшем использовании служебной информации ограниченного распространения принимает ликвидационная комиссия.

2. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения

2.1. Необходимость проставления пометки «Для служебного пользования» на документах и изданиях, содержащих служебную информацию ограниченного распро-

странения, определяется исполнителем и должностным лицом, подписывающим или утверждающим документ. Указанная пометка и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке и титульном листе издания, а также на первой странице сопроводительного письма к таким документам.

2.2. Прием и учет (регистрация) документов, содержащих служебную информацию ограниченного распространения, осуществляются, как правило, структурными подразделениями, которым поручен прием и учет несекретной документации.

2.3. Документы с пометкой «Для служебного пользования»:

- печатаются в машинописном бюро. На обороте последнего листа каждого экземпляра документа машинистка должна указать количество отпечатанных экземпляров, фамилию исполнителя, свою фамилию и дату печатания документа. Отпечатанные и подписанные документы вместе с черновиками и вариантами передаются для регистрации работнику, осуществляющему их учет. Черновики и варианты уничтожаются этим работником с отражением факта уничтожения в учетных формах;
- учитываются, как правило, отдельно от несекретной документации. При незначительном объеме таких документов разрешается вести их учет совместно с другими несекретными документами. К регистрационному индексу документа добавляется пометка «ДСП»;
- передаются работникам подразделений под расписку;
- пересылаются сторонним организациям фельдшерской связью, заказными или ценными почтовыми отправлениями;
- размножаются (тиражируются) только с письменного разрешения соответствующего руководителя. Учет размноженных документов осуществляется поэкземплярно;
- хранятся в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах).

2.4. При необходимости направления документов с пометкой «Для служебного пользования» в несколько адресов составляется указатель рассылки, в котором по-адресно проставляются номера экземпляров отправляемых документов. Указатель рассылки подписывается исполнителем и руководителем структурного подразделения, готовившего документ.

2.5. Исполненные документы с пометкой «Для служебного пользования» группируются в дела в соответствии с номенклатурой дел несекретного делопроизводства. При этом на обложке дела, в которое помещены такие документы, также проставляется пометка «Для служебного пользования».

2.6. Уничтожение дел, документов с пометкой «Для служебного пользования», утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

2.7. Передача документов и дел с пометкой «Для служебного пользования» от одного работника другому осуществляется с разрешения соответствующего руководителя.

2.8. При смене работника, ответственного за учет документов с пометкой «Для служебного пользования», составляется акт приема-сдачи этих документов, который утверждается соответствующим руководителем.

2.9. Проверка наличия документов, дел и изданий с пометкой «Для служебного пользования» проводится не реже одного раза в год комиссиями, назначаемыми приказом руководителя. В состав таких комиссий обязательно включаются работники, ответственные за учет и хранение этих материалов.

В библиотеках и архивах, где сосредоточено большое количество изданий, дел и других материалов с пометкой «Для служебного пользования», проверка наличия может проводиться не реже одного раза в пять лет.

Результаты проверки оформляются актом.

2.10. О фактах утраты документов, дел и изданий, содержащих служебную информацию ограниченного распространения, либо разглашения этой информации ставится в известность руководитель организации и назначается комиссия для расследования обстоятельств утраты

или разглашения. Результаты расследования докладываются руководителю, назначившему комиссию.

На утраченные документы, дела и издания с пометкой «Для служебного пользования» составляется акт, на основании которого делаются соответствующие отметки в учетных формах. Акты на утраченные дела постоянного срока хранения после их утверждения передаются в архив для включения в дело фонда.

2.11. При снятии пометки «Для служебного пользования» на документах, делах или изданиях, а также в учетных формах делаются соответствующие отметки и информируются все адресаты, которым эти документы (издания) направлялись.

ПРИЛОЖЕНИЕ 4

(рекомендуемое)

СОГЛАШЕНИЕ

о неразглашении коммерческой тайны

г. _____ « » _____ 20__ г.

_____ (далее — Организация),

(наименование организации, предприятия)

в лице ее руководителя _____

(должность, инициалы и фамилия руководителя)

действующего на основании _____

и гражданин _____

(фамилия, имя, отчество)

действующий от своего имени, в дальнейшем именуемые «сторонами», заключили настоящее Соглашение о нижеследующем:

1. _____ поставлен в известность
(инициалы и фамилия гражданина)

и согласен, что в качестве работника по роду своей трудовой деятельности (обязанностям) будет иметь доступ к коммерческой тайне организации и ее контрагентов (далее — коммерческая тайна).

2. _____ ознакомлен:

(инициалы и фамилия гражданина)

- с перечнем информации, составляющей коммерческую тайну;
- с установленным режимом коммерческой тайны и мерами ответственности за его нарушение.

3. Руководитель организации обязуется своевременно доводить до _____ все изменения

(инициалы и фамилия гражданина)

вносимые в перечень информации, составляющей коммерческую тайну, в режим коммерческой тайны и меры ответственности за его нарушение.

4. Руководитель организации обязуется создавать необходимые условия _____

(инициалы и фамилия гражданина)

для работы с информацией, составляющей коммерческую тайну.

5. _____ добровольно принимает

(инициалы и фамилия гражданина)

на себя следующие обязательства.

5.1. Выполнять установленный в организации режим коммерческой тайны.

5.2. Не разглашать информацию, составляющую коммерческую тайну и без согласия руководителя организации не использовать эту информацию в личных целях.

5.3. Не разглашать информацию, составляющую коммерческую тайну после прекращения трудового договора в течение _____ лет¹.

5.4. Возместить организации причиненный ущерб, в случае разглашения информации, составляющей коммерческую тайну организации.

5.5. Передать организации при прекращении (расторжении) трудового договора все имеющиеся материальные носители, содержащие информацию, составляющую коммерческую тайну.

6. _____ согласен на проведение

(инициалы и фамилия гражданина)

в отношении него проверочных мероприятий службой безопасности организации².

7. Срок действия настоящего Соглашения устанавливается со дня его подписания на весь период трудовых отношений работника с организацией (ее правопреемником).

8. Настоящее Соглашение составлено в единственном экземпляре, который подлежит хранению в личном деле работника до его увольнения и не менее _____ лет³ после его увольнения.

9. Условия настоящего Соглашения могут быть изменены в письменной форме только по взаимному соглашению сторон.

Подпись гражданина
(работника)

Должность и подпись
руководителя организации

(инициалы и фамилия)

(личная подпись)

(паспортные данные)

(инициалы и фамилия)

« » _____ 20__ г.

« » _____ 20__ г.

МП

Примечания:

¹ Как правило — трех лет.

² В объеме мероприятий, предусмотренных Федеральным законом «О частной детективной и охранной деятельности в Российской Федерации», при наличии у Службы безопасности соответствующей лицензии.

³ Как правило — трех лет, но не менее срока, указанного в пункте 5.3.

В Соглашение могут включаться и другие обязательства сторон, например, об информировании службы безопасности о фактах (попытках) получения третьими лицами информации, составляющей коммерческую тайну; о нарушениях режима коммерческой тайны (в том числе об утрате пропусков, ключей от сейфов или режимных помещений, личных номерных печатей) и т. д.

Форма № 4
(формат для журнала А4,
для карточки — А5)

ЖУРНАЛ (КАРТОЧКА) УЧЕТА

(вид документов)

(наименование организации или подразделения)

Порядковый №	Дата	Учетный № и гриф конфиденциальности	Заголовок	Кол-во экземпляров	Кол-во листов в экземпляре	Местонахождение
1	2	3	4	5	6	7

Форма № 5
(формат А3 в стиб)

ЖУРНАЛ УЧЕТА

ПОСТУПИВШИХ ДОКУМЕНТОВ

(наименование организации или подразделения)

Дата поступления пакета (документа)	№ реестра или подпись сдвигевого пакет (документ)	Откуда поступила	№ и гриф поступившего документа, дата издания	Входящий № документа (№ экз.) и гриф конфиденциальности	Вид и заголовок документа	Кол-во листов документа	Кол-во листов приложения
1	2	3	4	5	6	7	8

Продолжение формы № 5

Кому выдан	Кол-во листов	Подпись за получение и дата	Подпись за возврат и дата	Местонахождение (№ дела, №№ листов)	№ по учету выделенного хранения, кол-во листов	Примечание (отметка о возврате документа)
9	10	11	12	13	14	15

Форма № 6
(формат А5)

КАРТОЧКА КОНТРОЛЯ

ИСПОЛНЕНИЯ ДОКУМЕНТА

СРОК ИСПОЛНЕНИЯ _____

(учетный №, гриф конфиденциальности и дата документа)

Вид и заголовков документа	От кого поступил	Резолюция (должностное лицо и содержание)	Ответственный исполнитель	Контрольные отметки	Отметка о снятии с контроля
1	2	3	4	5	6

Форма № 7
(формат А3 в гиб)

ЖУРНАЛ УЧЕТА

КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ ВЫДЕЛЕННОГО ХРАНЕНИЯ

(наименование организации или подразделения)

Учетный (инв.) № и гриф конфиденциальности	Дата регистрации	Вид и заголовков документа	Откуда поступил (кем разработан)	С какого учетного номера	№№ экземпляров	Кол-во листов в экземпляре
1	2	3	4	5	6	7

Продолжение формы № 7

Местонахождение	Отметка о картотеке	Отметка об отрисовке	Отметка о возврате	Отметка о снятии с учета выделенного хранения	Отметка об уничтожении
8	9	10	11	12	13

Форма № 8
(формат А5)

КАРТОЧКА УЧЕТА

ВЫДАЧИ КОНФИДЕНЦИАЛЬНОГО ДОКУМЕНТА (ДЕЛА)

(учетный №, гриф конфиденциальности, наименование документа, количество листов)

Кому выдан документ	Кол-во листов	Подпись за получение и дата	Подпись за возврат и дата
1	2	3	4

Форма № 9
(формат А4)

ЖУРНАЛ УЧЕТА

КОПИРОВАНИЯ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

(наименование организации или подразделения)

Учетный №, гриф конфиденциальности и дата документа	Количество или номера страниц	Дата копирования	Кол-во снятых копий (листов или экземпляров)	Учетные №№, присвоенные копиям (экземплярам)	Отметка об уничтожении брака (кол-во листов / подпись)	Подпись за получение и дата
1	2	3	4	5	6	7

Форма № 10
(формат А4)

РЕЕСТР

**ВРЕМЕННО ПЕРЕДАВАЕМЫХ ДОКУМЕНТОВ,
ЗАРЕГИСТРИРОВАННЫХ ЗА**

(инициалы и фамилия)

Дата	Вид документа	Учетный № и гриф конфиденциальности	Кол-во листов	Подпись за получение документа и дата	Подпись за возврат документа и дата
1	2	3	4	5	6

ОПИСЬ ДОКУМЕНТОВ

НАХОДЯЩИХСЯ у _____

(инициалы и фамилия)

Порядко- вый №	Дата по- лучения до- кумента	Учетный № и гриф конфи- денциаль- ности документа	Вид или на- звание до- кумента	Кол-во листов	Отметка о возврате документа
1	2	3	4	5	6

ЖУРНАЛ ПЕРЕДАЧИ ПОД ОХРАНУ

ПОМЕЩЕНИЙ И ПЕНАЛОВ С КЛЮЧАМИ

(наименование организации или подразделения)

№ выдае- мого поме- щения	Дата и вре- мя пере- дачи под охрану	№ печати, которой опечатано помещение	№ печати, которой опечатан пенал с ключами	Подпись лица, передавшего помещение и пенал под охрану	Отметка о включе- нии сигна- лизации
1	2	3	4	5	6

Продолжение формы № 12

Подпись лица, принявшего по- мещение и пенал под охрану	Дата и время получения пенала с клю- чами	Подпись лица, получившего пенал	Отметка о выключении сигнализации	Примечание
7	8	9	10	11

**ЖУРНАЛ УЧЕТА
НАРУШЕНИЙ ПОРЯДКА ОБРАЩЕНИЯ
С КОНФИДЕНЦИАЛЬНЫМИ ДОКУМЕНТАМИ**

(наименование организации или подразделения)

Дата нарушения	Фамилия и инициалы лица, допустившего нарушение	Наименование структурного подразделения	Краткое изложение нарушения	Принятые меры, №№ приказов	№ и дата заключения внутреннего расследования
1	2	3	4	5	6

ПРИЛОЖЕНИЕ В

Порядок оформления конфиденциальных документов

Конфиденциальные документы должны быть оформлены установленным порядком.

Наиболее многочисленными по составу и объему являются документы, относящиеся к системе организационно-распорядительной документации. Поэтому порядок оформления конфиденциальных документов целесообразно рассмотреть на примере этой системы документации. Тем более что в отличие от открытых документов порядок оформления реквизитов для конфиденциальных организационно-распорядительных документов имеет ряд отличий.

Что касается конфиденциальных документов, входящих в другие системы документации, то их оформление отличается от открытых документов только проставлением грифа конфиденциальности и номеров экземпляров.

При подготовке и оформлении конфиденциальных и открытых организационно-распорядительных документов используют следующие реквизиты¹:

- 01 — Государственный герб Российской Федерации;
- 02 — герб субъекта Российской Федерации;

¹ ГОСТ Р 6.30 — 2003.

- 03 — эмблема организации или товарный знак (знак обслуживания);
- 04 — код организации;
- 05 — основной государственный регистрационный номер (ОГРН) юридического лица;
- 06 — идентификационный номер налогоплательщика / код причины постановки на учет (ИНН/КПП);
- 07 — код формы документа;
- 08 — наименование организации;
- 09 — справочные данные об организации;
- 10 — наименование вида документа;
- 11 — дата документа;
- 12 — регистрационный номер документа;
- 13 — ссылка на регистрационный номер и дату документа;
- 14 — место составления или издания документа;
- 15 — адресат;
- 16 — гриф утверждения документа;
- 17 — резолюция;
- 18 — заголовок к тексту;
- 19 — отметка о контроле;
- 20 — текст документа;
- 21 — отметка о наличии приложения;
- 22 — подпись;
- 23 — гриф согласования документа;
- 24 — визы согласования документа;
- 25 — оттиск печати;
- 26 — отметка о заверении копии;
- 27 — отметка об исполнителе;
- 28 — отметка об исполнении документа и направлении его в дело;
- 29 — отметка о поступлении документа в организацию;
- 30 — идентификатор электронной копии документа.

Для конфиденциальных документов, предусмотрено использование дополнительных реквизитов, таких как:

- гриф конфиденциальности документа;
- номер экземпляра документа;
- отметка о снятии копии с документа.

Каждый лист документа должен иметь поля: левое, верхнее и нижнее — размером не менее 20 мм; правое — не менее 10 мм.

В зависимости от расположения реквизитов бланки могут быть угловые или продольные.

Схема расположения реквизитов и границы зон документов на формате А4 для углового бланка прилагается.

Для организации, ее структурного подразделения, должностного лица установлены следующие виды бланков документов:

- общий бланк (используют для изготовления любых видов документов, кроме письма);
- бланк письма;
- бланк конкретного вида документа.

Общий бланк включает в себя реквизиты 01 (02 или 03), 08, 11, 14.

Бланк письма включает в себя реквизиты 01 (02 или 03), 04, 05, 06, 08, 09 и, при необходимости, ограничительные отметки для верхних границ зон расположения реквизитов 11, 12, 13, 14, 15, 17, 18, 19, 20.

Бланк конкретного вида документа (кроме письма) включает в себя реквизиты 01 (02 или 03), 08, 10, 14 и при необходимости ограничительные отметки для границ зон расположения реквизитов 11, 12, 13, 18, 19.

При расположении реквизитов на бланках документов необходимо учитывать, что реквизит 01 (02 или 03) располагают над серединой реквизита 08. Реквизит 03 допускается располагать на уровне реквизита 08.

Реквизиты 08, 09, 10, 14, ограничительные отметки для реквизитов 11, 12, 13 в пределах границ зон расположения реквизитов размещают одним из способов:

- центрированным (начало и конец каждой строки реквизитов равно удалены от границ зоны расположения реквизитов);
- флажковым (каждая строка реквизитов начинается от левой границы зоны расположения реквизитов).

При изготовлении документов на двух и более страницах вторую и последующие страницы нумеруют. Номера страниц проставляют посередине верхнего поля листа.

Различные реквизиты оформляют (проставляют) на разных этапах подготовки и обработки документов, в зависимости от их предназначения.

Рассмотрим подробнее требования к оформлению указанных реквизитов.

Государственный герб Российской Федерации (реквизит 01) — воспроизводят на бланках документов федеральных органов государственной власти, подведомственных им организаций, учреждений и предприятий, в соответствии с Федеральным конституционным законом «О Государственном гербе Российской Федерации».

Другие организации (предприятия) используют бланки без Государственного герба.

Герб субъекта Российской Федерации (реквизит 02) — воспроизводят на бланках документов в соответствии с правовыми актами субъектов Российской Федерации.

Эмблему организации или товарный знак (знак обслуживания) (реквизит 03) — воспроизводят на бланках организаций в соответствии с уставом (положением об организации). Эмблема представляет собой утвержденное установленным порядком символическое изображение, отражающее направление деятельности и (или) историю организации.

Под товарным знаком и знаком обслуживания понимаются зарегистрированные установленным порядком обозначения, служащие для индивидуализации товаров, выполняемых работ или оказываемых услуг юридических или физических лиц. Эти вопросы регулируются федеральным законом «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товара».

Код организации (реквизит 04) проставляют по Общероссийскому классификатору предприятий и организаций (ОКПО).

Основной государственный регистрационный номер (ОГРН) юридического лица (реквизит 05) и **идентификационный номер налогоплательщика/код причины постановки на учет (ИНН/КПП)** (реквизит 06) — проставляют в соответствии с документами, выдаваемыми налоговыми органами.

Код формы документа (реквизит 07) — проставляют по Общероссийскому классификатору управленческой документации (ОКУД).

Наименование организации (реквизит 08) — указывают наименование организации, являющейся автором документа. Оно должно точно соответствовать наименованию, закрепленному в ее учредительных документах. Если организация по учредительным документам имеет и сокращенное наименование, то оно помещается ниже полного или за ним (в скобках).

При наличии вышестоящей организации она указывается над наименованием данной организации в сокращенном, а при его отсутствии — в полном виде.

Наименование филиала, территориального отделения, представительства, структурного подразделения организации указывается в том случае, если они являются автором документа, и располагается ниже наименования организации.

Справочные данные об организации (реквизит 09) — могут включать: почтовый адрес, номер телефона и другие сведения по усмотрению организации (номера факсов, телексов, счетов в банке, адрес электронной почты и др.).

Наименование вида документа (реквизит 10) — должно соответствовать видам документов, предусмотренным ОКУД. В письме наименование вида документа не указывается.

Дата документа (реквизит 11) — дата подписания или утверждения документа. Документы, изданные двумя или более организациями, должны иметь одну (единую) дату.

Дату документа оформляют арабскими цифрами в последовательности: день месяца, месяц, год. День месяца и месяц оформляют двумя парами цифр, разделенными точкой, год — четырьмя цифрами, например:

05.06.2006.

Допускается также словесно-цифровой способ оформления даты, например:

05 июня 2006 г.

или оформление даты в последовательности: год, месяц, день месяца, например:

2006.06.05.

Регистрационный номер документа (реквизит 12) — состоит из его порядкового номера по учету, в который можно включать по усмотрению организации дополнительные индексы (сокращенную информацию для идентификации документа по видам учета).

Регистрационный номер конфиденциального документа проставляется на первом листе документа (в определенном для этого реквизита месте), на последнем листе в реквизите «Отметка об исполнителе», а также на остальных листах документа (если они есть) в левом нижнем поле лицевой стороны. При этом рядом с номером проставляется аббревиатурой гриф конфиденциальности документа, например:

№ 25 ДСП

или

№ 1/25-ДСП,

или

№ 50-КТ,

или

№ АВ/50-КТ.

Регистрационный номер документа, составленного совместно двумя и более организациями, состоит из регистрационных номеров документа каждой из этих организаций, проставляемых через наклонную черту в порядке указания авторов в документе, например:

№ 25/50-ДСП.

Ссылка на регистрационный номер и дату документа (реквизит 13) — включает в себя регистрационный номер и дату документа, на который дается ответ.

Следует иметь в виду, что на поступивший конфиденциальный документ ответный документ может быть как конфиденциальным, так и открытым, точно так же, как и на поступивший открытый документ, ответный документ может быть открытым или конфиденциальным. Гриф конфиденциальности документа определяется конфиденциальностью сведений, содержащихся в каждом конкретном документе.

Если ответ дается на конфиденциальный документ, то в ссылке на регистрационный номер к нему аббревиатурой добавляют гриф конфиденциальности, например:

На № 25-КТ от 05.06.2006.

Место составления или издания документа (реквизит 14) указывают в том случае, если затруднено его определение по реквизитам «Наименование организации» и «Справочные данные об организации». Как правило, этот реквизит проставляют в актах, протоколах и в ряде других документов. Место составления или издания указывают с учетом принятого административно-территориального

деления, используя только общепринятые сокращения, например:

г. Москва

или

пос. Северный.

Гриф конфиденциальности документа (дополнительный реквизит) — включает в себя непосредственно гриф конфиденциальности (по виду тайны), который указывают полностью (без аббревиатур и сокращений) и без кавычек, в правом верхнем углу документа, например:

Для служебного пользования

или

Коммерческая тайна.

Под грифом конфиденциальности документа, при необходимости, может проставляться срок действия конфиденциальности.

Номер экземпляра документа (дополнительный реквизит) — проставляют на конфиденциальных документах в целях учета каждого экземпляра документа, для контроля его движения и местонахождения. Реквизит оформляется следующим образом:

Экз. № ___

(без кавычек) с проставлением на каждом экземпляре его номера. Если документ подготовлен в одном экземпляре, то проставляется:

Экз. единственный

или

Экз. единств.

Реквизит помещается на первом листе ниже срока конфиденциальности, а при отсутствии срока конфиденциальности — под грифом конфиденциальности.

Адресат (реквизит 15) — включает указание о получателе документа. В качестве адресата могут быть организации, их структурные подразделения, должностные или физические лица. Физические лица применительно к конфиденциальным документам адресатами быть не должны, поскольку не могут в должной мере обеспечить сохранность и конфиденциальность документов. Наименование организации и ее структурного подразделения указывают в именительном падеже. Например:

*Генеральный штаб Вооруженных Сил
Российской Федерации*

При адресовании документа должностному лицу инициалы указывают перед фамилией.

Должность лица, которому адресован документ, указывают в дательном падеже, например:

*Генеральному директору
ОАО «Восток»
И.И. Иванову*

или

*АО «Север»
Главному энергетiku
И.И. Иванову.*

Если документ отправляют в несколько однородных организаций или в несколько структурных подразделений одной организации, то их следует указывать обобщенно, например:

*Начальникам отделов
АО «Восток».*

Документ не должен содержать более четырех адресатов. Слово «Копия» перед вторым и последующими адресатами не указывают. При большем числе адресатов составляют список (расчет) рассылки документа, а в реквизите «адресат» указывается их обобщенное название.

В состав реквизита может входить почтовый адрес. Элементы почтового адреса указывают в последовательности, установленной правилами оказания услуг почтовой связи. При адресовании письма в организацию указывают ее наименование, а затем почтовый адрес, например:

*АО «Северо-восток»
123456, г. Москва, ул. Московская, д. 10.*

При адресовании документа физическому лицу указывают фамилию и инициалы получателя, затем почтовый адрес, например:

*Иванову И.И.
123456, г. Москва,
ул. Московская, д. 10, кв. 20.*

Допускается центрировать строки этого реквизита, например:

*ЗАО «Северо-запад»
123456, г. Москва, ул. Московская, д. 10.*

В случае необходимости при адресовании документа должностному лицу (должностным лицам) проставляют пометку «Лично».

Такая пометка имеет двоякое содержательное значение.

В первом случае — это указание на необходимость первоначального рассмотрения документа лицом, которому он адресован (в этом значении пометка не имеет отношения к ограничению доступа к документу и может проставляться как на конфиденциальных, так и на открытых документах).

Во втором случае — это указание на возможность работы с документом или его последующего переадресования только лицом, которому он адресован, что является составной частью ограничения доступа к документу.

Для различия значений этой пометки в первом значении она проставляется под адресатом или после адресата (в скобках без кавычек), во втором значении — над адресатом или перед адресатом (без скобок и кавычек). Во втором значении пометка проставляется и на конверте (пакете), в котором пересылается документ и он вскрывается только лицом, которому адресован.

В качестве ограничения доступа к конфиденциальному документу также может быть использована пометка «Только:».

Порядок применения пометок ограничения доступа к конфиденциальному документу должен быть регламентирован системой доступа к конфиденциальным документам (см. главу 4).

Гриф утверждения документа (реквизит 16) — документ утверждается должностным лицом (должностными лицами) или специально издаваемым документом. При утверждении документа должностным лицом гриф утверждения документа должен состоять из слова УТВЕРЖДАЮ (без кавычек), наименования должности лица, утверждающего документ, его подписи, инициалов, фамилии и даты утверждения, например:

УТВЕРЖДАЮ
 Президент ЗАО «Север»
 личная подпись И.И. Иванов
 05.06.2006.

При утверждении документа несколькими должностными лицами их подписи располагают на одном уровне.

При утверждении документа постановлением, решением, приказом, протоколом гриф утверждения состоит из слова УТВЕРЖДЕН (УТВЕРЖДЕНА, УТВЕРЖДЕНЫ

или УТВЕРЖДЕНО), наименования утверждающего документа в творительном падеже, его даты и номера. Допускается центрировать строки этого реквизита.

Например:

УТВЕРЖДЕН
решением общего собрания
акционеров от 05.06.2006 № 25

или

УТВЕРЖДЕНО
приказом директора АО «Восток»
от 05.06.2006. № 50.

Резолюция (реквизит 17), пишется на полученном документе соответствующим должностным лицом и включает в себя инициалы и фамилии, исполнителей, содержание поручения (при необходимости), срок исполнения, подпись и дату, например:

И.И. Иванову
П.П. Петрову
Прошу подготовить проект
договора к 05.10.2006.
личная подпись
05.06.2006.

Допускается оформлять резолюцию на отдельном листе или внизу документа (в случае последующей резолюции или при переадресовании документа по исполнителям), на свободном месте (см. гл. X).

Заголовок к тексту (реквизит 18) — является кратким содержанием документа. Заголовок должен быть согласован с наименованием вида документа и может отвечать на вопросы: *О чем? (О ком?)*, например:

*Приказ о создании аттестационной комиссии
или Чего? (Кого?)*, например:
Должностная инструкция ведущего инженера.

К тексту документов, оформленных на бланках формата А5, заголовок допускается не указывать.

Отметка о контроле (реквизит 19) — при взятии документа на контроль (за его исполнением) на нем проставляют отметку (как правило, штампом) в виде слова «Контроль» или буквы «К» (см. гл. X).

Текст документа (реквизит 20) — составляют на русском языке или на государственных языках субъектов Российской Федерации (в соответствии с законодатель-

ством Российской Федерации и субъектов Российской Федерации). В коммерческих организациях текст документа может составляться и на иных языках, предусмотренных договорами между организациями.

Тексты документов оформляют в виде анкеты, таблицы, связного текста или в виде соединения этих структур.

При составлении текста в виде анкеты наименования признаков характеризуемого объекта должны быть выражены именем существительным в именительном падеже или словосочетанием с глаголом второго лица множественного числа настоящего или прошедшего времени («имеете», «владеете» или «были», «находились» и т. д.). Характеристики, выраженные словесно, должны быть согласованы с наименованиями признаков.

Графы и строки таблицы должны иметь заголовки, выраженные именем существительным в именительном падеже. Подзаголовки граф и строк должны быть согласованы с заголовками. Если таблицу печатают более чем на одной странице, графы таблицы должны быть пронумерованы и на следующих страницах допускается печатать только номера этих граф.

Таблицы также должны иметь заголовки, над которыми справа пишется слово «Таблица» и указывается ее порядковый номер. (Если таблица одна, то номер не представляется). На все таблицы в тексте документа даются ссылки.

Связный текст, как правило, структурно состоит из двух частей. В первой части указывают причины, основания, цели составления документа, во второй (заключительной) — решения, выводы, просьбы, предложения, рекомендации. Текст может содержать одну часть (например, приказы — распорядительную часть без констатирующей; письма, заявления — просьбу без пояснения).

В тексте документа, подготовленного на основании документов других организаций или ранее изданных документов, указывают их реквизиты: наименование документа, наименование организации — автора документа, дату документа, регистрационный номер документа, заголовок к тексту. В этом случае, как правило, делается ссылка «Основание:». Если основанием является конфиденциальный документ, то к его номеру аббревиатурой добавляется гриф конфиденциальности.

Если текст содержит несколько решений, выводов и т. д., то его можно разбивать на разделы, подразделы, пункты, которые нумеруют арабскими цифрами, например:

1.2.3.

или

2.5.

В документах (приказ, распоряжение и т. д.) организаций, действующих на принципах единоначалия, а также документах, адресованных руководству организации, текст излагают от первого лица единственного числа («приказываю», «предлагаю», «прошу»).

В документах коллегиальных органов текст излагают от третьего лица единственного числа («постановляет», «решил»).

В совместных документах текст излагают от первого лица множественного числа («приказываем», «решили»).

Текст протокола излагают от третьего лица множественного числа («слушали», «выступили», «постановили», «решили»).

В документах, устанавливающих права и обязанности организаций, их структурных подразделений (положение, инструкция), а также содержащих описание, оценку фактов или выводы (акт, справка), используют форму изложения текста от третьего лица единственного или множественного числа («отдел осуществляет функцию», «в состав объединения входят», «комиссия установила»).

В письмах используют следующие формы изложения:

- от первого лица множественного числа («просим направить», «направляем на рассмотрение»);
- от первого лица единственного числа («считаю необходимым», «прошу выделить»);
- от третьего лица единственного числа («министерство не возражает», «собрание считает возможным»).

Для однотипных конфиденциальных документов допускается изготавливать их типовые формы, представляющие собой бланки с напечатанным текстом, содержащим постоянно повторяющуюся открытую информацию и имеющим в соответствующих местах пропуски для последующего внесения конфиденциальной информации. Такие формализованные бланки существенно сокращают

время на подготовку конкретных документов, так как не требуют составления черновика документа.

Отметка о наличии приложения (реквизит 21) — к конфиденциальному документу оформляется в зависимости от того, названо приложение в тексте или нет и конфиденциальное оно или открытое.

Если приложение названо в тексте, то в отметке о наличии приложения его название не указывается, если не названо — указывается.

Кроме того, если приложение конфиденциальное, то в отметке о наличии приложения проставляют его учетный номер и гриф конфиденциальности (полностью), номер (номера) экземпляров, количество листов в экземпляре; если приложение открытое — только количество листов в экземпляре и количество экземпляров. При наличии нескольких приложений они нумеруются.

Например, отметка о наличии приложения в конфиденциальном документе может быть оформлена следующим образом:

*Приложение: № 10, для служебного пользования,
экз. № 2 на 6 л.,*

или

Приложение: упомянутое по тексту, на 6 л.,

или

*Приложения: 1. Справка о реализации продукции,
№ 20, коммерческая тайна,
экз. № 1, 2 на 10 л. каждый.
2. Акт о списании изделий, на 3 л.,
в 2-х экз. каждый.*

Если приложение сброшюровано, то указывается количество экземпляров брошюр (книг).

При направлении приложения не во все указанные в документе адреса, в конце отметки о его наличии это оговаривается особо, например:

— только в первый адрес.

Если к документу прилагают другой документ, также имеющий приложение, отметку о наличии приложения оформляют следующим образом:

*Приложение: письмо РГГУ от 05.06.2006. № 50-ДСП
и приложение к нему, всего на 3 л.*

В приложении к распорядительному документу в правом верхнем углу первого листа пишется: Приложение (без кавы-

чек) с указанием наименования распорядительного документа, его даты, номера и грифа конфиденциальности, например:

*Приложение
к приказу председателя правления
от 05.06.2006 № 25-КТ.*

При наличии нескольких приложений к распорядительному документу на каждом из них проставляется порядковый номер: Приложение 1, Приложение 2 и т. д. Допускается слово «ПРИЛОЖЕНИЕ» печатать прописными буквами, ставить перед его порядковым номером знак «№», а также центрировать строки этого реквизита.

В приложении к распорядительному документу (постановления, приказы, распоряжения, правила, инструкции, положения, решения) на первом его листе в правом верхнем углу пишут «Приложение №» с указанием наименования распорядительного документа, его даты и регистрационного номера, например:

*Приложение 2
к приказу по РГГУ
от 05.06.2006 № 25-ДСП*

или

ПРИЛОЖЕНИЕ № 2
*к протоколу
от 05.06.2006 № 50-ДСП.*

Подпись (реквизит 22) — имеет в своем составе: наименование должности лица, подписавшего документ (полное, если документ оформлен не на бланке документа, и сокращенное — на документе, оформленном на бланке); личная подпись; расшифровка подписи (инициалы, фамилия), например:

*Вице-президент Ассоциации
региональных предприятий* *личная подпись* *И.И. Иванов*

или на бланке:

Вице-президент *личная подпись* *И.И. Иванов*

Допускается в реквизите «Подпись» центрировать наименование должности лица, подписавшего документ, например:

Исполнительный директор
ЗАО «Запад» *личная подпись* *И.И. Иванов*

При оформлении документа на бланке должностного лица должность этого лица в подписи не указывают.

При подписании документа несколькими должностными лицами их подписи располагают одну под другой в последовательности, соответствующей занимаемой должности, например:

<i>Директор института</i>	<i>личная подпись</i>	<i>И.И. Иванов</i>
<i>Главный бухгалтер</i>	<i>личная подпись</i>	<i>П.П. Петров</i>

При подписании документа несколькими лицами равных должностей их подписи располагают на одном уровне, например:

<i>Заместитель директора по научной работе</i>	<i>Заместитель директора по безопасности</i>	
<i>личная подпись И.И. Иванов</i>	<i>личная подпись П.П. Петров</i>	

При подписании совместного документа первый лист оформляют не на бланке.

В документах, составленных комиссией, указывают не должности лиц, подписывающих документ, а их обязанности в составе комиссии, например:

<i>Председатель комиссии</i>	<i>личная подпись</i>	<i>И.И. Иванов</i>
<i>Члены комиссии</i>	<i>личная подпись</i>	<i>К.К. Кузнецов</i>
	<i>личная подпись</i>	<i>П.П. Петров</i>
	<i>личная подпись</i>	<i>С.С. Сидоров</i>

(в алфавитном порядке).

Гриф согласования документа (реквизит 23) — состоит из слова СОГЛАСОВАНО, должности лица, с которым согласован документ (включая наименование организации), личной подписи, расшифровки подписи (инициалов, фамилии) и даты согласования, например:

СОГЛАСОВАНО
 Генеральный директор
 АОЗТ «Север»
 личная подпись *И.И. Иванов*
 05.06.2006.

Допускается центрировать строки этого реквизита.

Если согласование осуществляют письмом, протоколом и др., гриф согласования оформляют следующим образом:

СОГЛАСОВАНО
 Письмо Российской академии
 военных наук
 от 05.06.2006 № 50-ДСП

ИЛИ

СОГЛАСОВАНО

Протокол заседания Правления
страховой компании «Юг»
от 05.06.2006 № 10-КТ.

Визы согласования документа (реквизит 24) — согласование документа оформляют визой, включающей в себя подпись и должность лица, визирующего документ, расшифровку подписи (инициалы, фамилию) и дату подписания, например:

Начальник юридического отдела
личная подпись И.И. Иванов
05.06.2006.

При наличии замечаний к документу визу оформляют следующим образом:

Замечания прилагаются
Начальник юридического отдела
личная подпись И.И. Иванов
05.06.2006.

Замечания излагают на отдельном листе, подписывают и прилагают к документу.

Для документа, подлинник которого остается в организации, визы проставляют в нижней части оборотной стороны последнего листа подлинника документа. Для документа, подлинник которого отправляют из организации, визы проставляют в нижней части лицевой стороны копии отправляемого документа.

Возможно оформление виз документа на отдельном листе согласования. Допускается, по усмотрению организации, подлистное визирование документа и его приложения.

Оттиск печати (реквизит 25) — печатью организации заверяют подлинность подписи должностного лица на документах, удостоверяющих права лиц, фиксирующих факты, связанные с финансовыми средствами, а также на иных документах, предусматривающих заверение подлинности подписи.

Отметка о заверении копии (реквизит 26) — при заверении соответствия копии документа подлиннику ниже реквизита «Подпись» проставляют заверительную надпись: «Верно», должность лица, заверившего копию, личную подпись, расшифровку подписи (инициалы, фамилию) и дату заверения, например:

Верно
Инспектор отдела кадров личная подпись И.И. Иванов
05.06.2006.

Допускается копию документа заверять печатью (или штампом).

Отметка об исполнителе (реквизит 27) — для конфиденциального документа является обязательным реквизитом и включает в себя: учетный номер и гриф конфиденциальности документа, количество изготовленных экземпляров, фамилию и инициалы исполнителя документа, фамилию и инициалы лица, печатавшего документ (если они разные), дату печатания документа и (при отправке документа в другие организации) номер его телефона. На внутренних документах допускается инициалы не указывать. Отметку об исполнителе располагают на лицевой или оборотной стороне последнего листа документа в левом нижнем углу, например:

№ 25-КТ

Отп. 2 экз.

Исп. Иванов И.И.

Отп. Петров П.П.

05.06.2006.

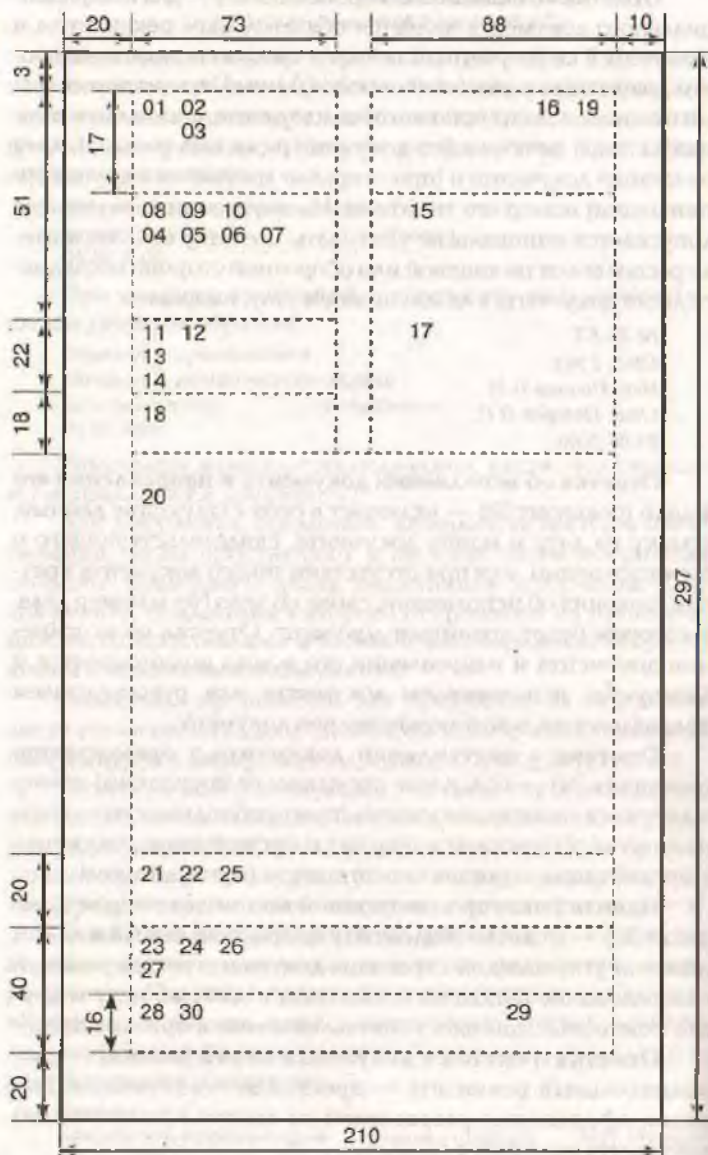
Отметка об исполнении документа и направлении его в дело (реквизит 28) — включает в себя следующие данные: ссылку на дату и номер документа, свидетельствующего о его исполнении, или при отсутствии такого документа краткие сведения об исполнении; слова «В дело №» и номер дела, в котором будет храниться документ. Отметка об исполнении документа и направлении его в дело подписывается и датируется исполнителем документа или руководителем подразделения, в котором исполнен документ.

Отметка о поступлении документа в организацию (реквизит 29) — содержит порядковый (входящий) номер и дату поступления документа (при необходимости — часы и минуты). Допускается отметку о поступлении документа в организацию проставлять штампом (нумератором).

Идентификатор электронной копии документа (реквизит 30) — отметка (колонтитул), проставляемый в левом нижнем углу каждой страницы документа и содержащий наименование файла на магнитном носителе, дату и другие поисковые данные, устанавливаемые в организации.

Отметка о снятии с документа копии (копий) — (дополнительный реквизит) — проставляется штампом. Порядок оформления разрешения на снятие копии (копий) документа изложен в гл. IX.

СХЕМА РАСПОЛОЖЕНИЯ РЕКВИЗИТОВ И ГРАНИЦ ЗОН
НА ФОРМАТЕ А4 УГЛОВОГО БЛАНКА



Учебное издание

Некраха Андрей Вячеславович
Шевцова Галина Александровна

**ОРГАНИЗАЦИЯ КОНФИДЕНЦИАЛЬНОГО
ДЕЛОПРОИЗВОДСТВА
И ЗАЩИТА ИНФОРМАЦИИ**

Компьютерная верстка

Е. Костраменкова

Корректоры

А. Греков

М. Яковлева

ООО «Академический Проект»

Изд. лиц. № 04050 от 20.02.01.

111399, Москва, ул. Маргеновская, 3.

Санитарно-эпидемиологическое заключение

Департамента государственного

эпидемиологического надзора

№ 71.99.02.953.Д.060321.01.06 от 23.01.06.

*По вопросам приобретения книги просим обращаться
в ООО «Тригиста»:*

111399, Москва, ул. Маргеновская, 3.

Тел.: (495) 305 3702; 305 6092; факс: 305 6088

E-mail: info@aproject.ru

www.aproject.ru

Подписано в печать с готовых диапозитивов 26.03.07.

Формат 84×108¹/₃₂. Гарнитура Балтика. Бумага писчая.

Печать офсетная. Усл. печ. л. 11,76. Тираж 3000 экз.

Заказ № 227.

Отпечатано в полном соответствии с качеством предоставленных

диапозитивов в ОАО «ИПП «Уральский рабочий»

620041, ГСП-148, Екатеринбург, ул. Тургенева, 13

http://www.uralprint.ru

e-mail: book@uralprint.ru

КНИГА — ПОЧТОЙ

Издательско-книготорговая фирма
«ТРИКСТА»

предлагает заказать и получить по почте книги
следующей тематики:

- › психология
- › философия
- › история
- › социология
- › культурология
- › учебная и справочная литература
по гуманитарным дисциплинам
для вузов, лицеев и колледжей

Прислав маркированный конверт с обратным адресом,
Вы получите каталог, информационные материалы
и условия рассылки.

Наш адрес:

111399, Москва, ул. Мартеновская, 3,
ООО «Трикста», служба «Книга — почтой».

Заказать книги можно также
по тел.: (495) 305-37-02, факсу: 305-60-88

или по электронной почте:

e-mail: info@aproject.ru

Просим Вас быть внимательными и указывать полный
почтовый адрес и телефон/факс для связи.
С каждым выполненным заказом Вы будете получать
информацию о новых поступлениях книг.
ЖДЕМ ВАШИХ ЗАКАЗОВ!

ИЗДАТЕЛЬСТВО «АКАДЕМИЧЕСКИЙ ПРОЕКТ»

ПРЕДСТАВЛЯЕТ НОВУЮ СЕРИЮ

«СОЦИОЛОГИЧЕСКИЕ ТЕХНОЛОГИИ»

ИНФОРМАЦИОННЫЕ
ВОЙНЫ В БИЗНЕСЕ
И ПОЛИТИКЕ.

ТЕОРИЯ И МЕТОДОЛОГИЯ

В.В. Цыганов, С.Н. Бухарин

Наше время — время новых наук. Дисциплины возникают как синтез ряда научных направлений (в данном случае социокультурной антропологии и социологии), как удовлетворение общественной потребности в новом типе и качестве знания.

Неизбежность становления и развития социологии культуры предопределена новым качеством развития общества, усилением культурной детерминанты в общественной жизни, интегрирующим значением культурной традиции, необходимостью изучения и управления процессом культурного развития.

Учебник предназначен для студентов гуманитарных специальностей.

Издательство «АКАДЕМИЧЕСКИЙ ПРОЕКТ»
ПРЕДСТАВЛЯЕТ НОВУЮ СЕРИЮ
«СОЦИОЛОГИЧЕСКИЕ ТЕХНОЛОГИИ»

МЕТОДЫ И ТЕХНОЛОГИИ ИНФОРМАЦИОННЫХ ВОЙН

С.Н. Бухарин, В.В. Цыганов

Излагаются методы и технологии информационных войн, основанные на их теории и методологии, а также практические применения. На основе изучения целей информационных войн спроектированы процедуры ситуационного анализа и алгоритмы определения стратегий информационного противоборства (в том числе провокаций). Разработаны процедуры планирования информационных операций, алгоритмы принятия решений в информационных войнах и подходы к управлению информационным противоборством. Эти методы и технологии использованы для анализа и проектирования комплексных систем управления противоборством в информационных войнах разной природы и масштаба — от корпоративных и отраслевых до региональных и национальных. Исследованы экологические информационные войны в условиях глобализации.

Книга предназначена руководителям и специалистам по информационному противоборству. Она ориентирована на ученых и специалистов по управлению, социологии, политологии, экономике, профессорско-преподавательскому составу и студентам социально-экономических факультетов, а также читателям, интересующимся проблемами информационных противоборств.

