Кришталюк А.Н.

КОНФИДЕНЦИАЛЬНОЕ ДЕЛОПРОИЗВОДСТВО И ЗАЩИТА КОММЕРЧЕСКОЙ ТАЙНЫ

курс лекций

Академия МАБИВ
www.mabiv.ru

Александр Кришталюк

Конфиденциальное делопроизводство и защита коммерческой тайны

МОО "Межрегиональная общественная организация "Академия безопасности и выживания""

2014

Кришталюк А. Н.

Конфиденциальное делопроизводство и защита коммерческой тайны / А. Н. Кришталюк — МОО "Межрегиональная общественная организация "Академия безопасности и выживания"", 2014

Конфиденциальное делопроизводство распространяется на документы, которые содержат в себе сведения, составляющие коммерческую и служебную тайну. Коммерческая тайна прямо связана с коммерческой деятельностью, является необходимым условием ее существования.Предназначено для преподавателей и студентов вузов специальностей по направлению безопасности, специалистов по безопасности, менеджеров и руководителей компаний.

Содержание

Александр Николаевич Кришталюк Конфиденциальное делопроизводство и защита коммерческой тайны. Курс лекций

А. Н. Кришталюк, руководитель Национального социального проекта «Здоровая Нация», аспирант кафедры «Туризм, рекреация и спорт» ФГБОУ ВПО «Госуниверситет – УНПК»

Введение

В русском языке общепринято, что слово «конфиденциальный» означает «не подлежащий оглашению, секретный».

Конфиденциальное делопроизводство распространяется на документы, которые содержат в себе сведения, составляющие коммерческую и служебную тайну. Коммерческая тайна прямо связана с коммерческой деятельностью, является необходимым условием ее существования.

Синонимом коммерческой деятельности является предпринимательская деятельность. Согласно Гражданскому кодексу Российской Федерации, предпринимательская деятельность – это «самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг лицами, зарегистрированными в этом качестве в установленном порядке». Следовательно, коммерческими предприятиями являются те, для которых извлечение прибыли является основной целью деятельности. Ими могут быть как частные, так и государственные, а также муниципальные предприятия.

Предпринимательскую деятельность могут осуществлять и некоммерческие предприятия, т. е. такие, которые в качестве основной цели имеют не извлечение прибыли, а достижение общественных благ: социальных, культурных, образовательных, здравоохранительных, благотворительных и др. Однако такие предприятия могут осуществлять предпринимательскую деятельность лишь постольку, поскольку это служит достижению целей, ради которых они созданы, и соответствующую этим целям. Отличительным признаком коммерческой деятельности является соизмерение затрат и результатов работы, получение максимальной прибыли.

Еще одной отличительной особенностью коммерческой деятельности является то, что она, как правило, осуществляется в условиях конкуренции, соперничества, борьбы предприятий за получение выгод, преимуществ по сравнению с предприятиями аналогичного профиля.

Коммерческая деятельность может осуществляться и при отсутствии конкурентов, при монопольном положении предприятия в той или другой сфере деятельности, однако это, скорее, исключение, чем правило. Правилом же является то, что конкурентная борьба – спутник коммерческой деятельности и условие выживания коммерческих предприятий. Отсюда – стремление сохранить в секрете от конкурентов (соперников) те приемы и особенности своей деятельности, которые обеспечивают преимущество над ними, отсюда и стремление конкурентов выявить эти секреты, чтобы использовать их в своих интересах.

Получение, использование, разглашение таких секретов без согласия их владельцев отнесены законодательством к одной из форм недобросовестной конкуренции, называемой промышленным шпионажем. Защищаемые секреты коммерческой деятельности получили название коммерческой тайны.

Информация, составляющая коммерческую тайну, – научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, в том числе ноу-хау, которая обладает действительной или потенциальной коммерческой ценностью в силу ее неизвестности третьим лицам, которые могли бы получить выгоду от ее разглашения или использования, к которой нет свободного доступа на законном основании и по отношению к которой принимаются адекватные ее ценности правовые, организационные, технические или иные меры охраны.

В свою очередь служебная тайна – это вид тайны, включающий полученную федеральными и муниципальными органами власти информацию, составляющую коммерческую тайну других субъектов, а также устанавливаемую и защищаемую органами власти и предприятиями собственную информацию, доступ к которой ограничивается служебной необходимостью.

Таким образом, коротко можно охарактеризовать коммерческую тайну как совокупность не являющихся государственной тайной сведений, представляющих действительную или потенциальную ценность для субъекта предпринимательства, разглашение которых может нанести ему ущерб и, в отношении которых приняты надлежащие меры по сохранению конфиденциальности.

Как видно из вышеуказанного определения одним из основных признаков сведений, составляющих коммерческую тайну, является то, что в отношении этих сведений приняты меры по обеспечению конфиденциальности. Только при соблюдении этих условий может наступить предусмотренная законодательством дисциплинарная, материальная, административная и уголовная ответственность.

Исходя из этого положения, даже если сведения связаны с производством, технологией, управлением, финансовой и другой деятельностью вашего предприятия и их разглашение может нанести вам ущерб, но в отношении них вы не предприняли меры по сохранению тайны, то вы не можете рассчитывать на их правовую защиту. И, таким образом, лица, незаконно завладевшие вашей коммерческой тайной, не будут нести никакой юридической ответственности. И это, в принципе, справедливо, почему государство должно защищать ваши тайны, если вы сами не предпринимаете никаких мер по их защите? Вот почему необходимо на каждом предприятии с самого начала его деятельности разработать систему по обеспечению сохранности коммерческой тайны.

Организация и технология конфиденциального делопроизводства не регламентированы государственными нормативными актами. Их должен определять обладатель конфиденциальных документов, учитывая специфику деятельности предприятия. Однако при этом ему необходимую руководствоваться определенными нормами и правилами работы с конфиденциальными документами, обеспечивающими нужный уровень функционирования предприятия, сохранность документов и конфиденциальность содержащейся в них информации.

Нужно помнить, что чем быстрее эти меры будут разработаны, тем быстрее сведения, составляющие коммерческую тайну вашего предприятия, подпадут под правовую защиту. Этим вы обезопасите себя от недобросовестной конкуренции со стороны ваших конкурентов.

Лекция 1. Сущность, задачи и особенности конфиденциального делопроизводства и защиты коммерческой тайны

По уровню доступности документы подразделяются на две категории:

– общедоступные;

– с ограниченным доступом.

Общедоступными являются открытые документы. К документам с ограниченным доступом относятся документы, работа с которыми может производиться по специальному разрешению уполномоченных на то лиц. Документирование открытой информации и организация работы с открытыми документами входят в сферу действия открытого делопроизводства. Документы с ограниченным доступом относятся к сфере деятельности не одного, а нескольких типов делопроизводства, в зависимости от того, к какому виду тайны относится содержащаяся в документах информация. Нормативными документами установлено *шесть видов тайны*:

– государственная;

– коммерческая;

– служебная;

– личная;

– семейная;

– профессиональная.

Документы, содержащие государственную тайну, относятся к сфере секретного делопроизводства. Документы, содержащие личную и различные подвиды профессиональной тайны, являются предметом соответствующих типов специального делопроизводства.

Конфиденциальное делопроизводство, как уже было отмечено, распространяется на документы, содержащие коммерческую и служебную тайну. При этом к документам, составляющим служебную тайну, отнесены только документы с грифом «Для служебного пользования», т. к. документы, содержащие коммерческую тайну других субъектов, должны обрабатываться и защищаться в режиме коммерческой тайны. Объединение конфиденциальных документов, содержащих коммерческую и служебную тайну, одним делопроизводством обусловлено тем, что эти документы почти полностью идентичны по технологическим процедурам составления, обработки, обращения, хранения и защиты.

Доступ к коммерческой тайне имеют работники, круг которых определен субъектом предпринимательства. Государственные контролирующие и правоохранительные органы в соответствии с полномочиями, предоставленными им законодательством по контролю и надзору, имеют право, в пределах своей компетенции, на основании письменного заявления знакомиться со сведениями, являющимися коммерческой тайной и составлять соответствующие акты изъятия документов, свидетельствующих о нарушении законодательства. При этом должностные лица этих органов несут предусмотренную законодательством ответственность за разглашение сведений, составляющих коммерческую тайну хозяйствующего субъекта.

Важным моментом является то, что иные органы и организации, в том числе средства массовой информации, правом истребования у хозяйствующего субъекта сведений, составляющих коммерческую тайну, не обладают.

Итак, какого рода сведения составляют коммерческую тайну? Вот лишь примерный список тех, которые содержат такие сведения:

– Производство;

– Управление;

– Планы;

– Финансы;
– Рынок;
– Партнеры;
– Переговоры;
– Контракты;
– Цены;
– Торги, аукционы;
– Наука и техника;
– Технология;
– Совещание;
– Безопасность.

Каждая из этих тем, в зависимости от специфики конкретного предприятия, может содержать различную информацию. В каждом случае эти сведения определяются индивидуально.

Важно, при определении объектов, которые составляют вашу коммерческую тайну, не включить в их список объектов, которые не могут составлять коммерческую тайну в соответствии с законодательством.

К *объектам коммерческой тайны* не могут относиться:

– учредительные документы, а также документы, дающие право на занятие предпринимательской деятельностью и отдельными видами хозяйственной деятельности, подлежащей лицензированию;

– сведения по утвержденным формам статистической отчетности, а также отчетности о финансово-экономической деятельности и иные данные, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей;

– документы об уплате налогов и других обязательных платежей;

– документы, удостоверяющие платежеспособность;

– сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

– сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении правил охраны труда, реализации продукции, причиняющей вред здоровью потребителей, а также о других нарушениях законодательства и размерах причиненного при этом ущерба.

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 учет, размножение, прохождение, исполнение, отправление, классификация, систематизация, подготовка для архивного хранения, уничтожение, режим хранения и обращения, проверки наличия.

По сфере деятельности открытое делопроизводство распространяется на управленческие действия и включает в основном управленческие документы. Конфиденциальное делопроизводство в силу условий работы с конфиденциальными документами распространяется как на управленческую, так и на различные виды производственной деятельности, включает не только управленческие, но и научно-технические документы (научно-исследовательские, проектные, конструкторские, технологические и др.). Кроме того, конфиденциальное делопроизводство распространяется не только на официальные документы, но и на их проекты, различные рабочие записи, не имеющие всех необходимых реквизитов, но содержащие информацию, подлежащую защите.

По видам работ конфиденциальное делопроизводство отличается от открытого, с одной стороны, большим их количеством, с другой – содержанием и технологией выполнения многих видов.

Помимо этого, третья составляющая конфиденциального делопроизводства – защита содержащейся в конфиденциальных документах информации – вообще не предусмотрена в определении открытого делопроизводства, хотя определяемая собственником часть открытой информации должна защищаться от утраты. Конфиденциальная информация должна защищаться и от утраты, и от утечки.

Термин «утечка конфиденциальной информации», вероятно, не самый благозвучный, однако он более емко, чем другие термины, отражает суть явления, к тому же он давно уже закрепился в научной литературе и нормативных документах. Утечка конфиденциальной информации представляет собой неправомерный, т. е. неразрешенный выход такой информации за пределы защищаемой зоны ее функционирования или установленного круга лиц, имеющих право работать с ней, если этот выход привел к получению информации (ознакомлению с ней) лицами, не имеющими к ней санкционированного доступа, независимо от того, работают или не работают такие лица на данном предприятии обусловлены уязвимостью информации.

Уязвимость информации следует понимать как ее доступность для дестабилизирующих воздействий, т. е. таких воздействий, которые нарушают установленный статус информации. Нарушение статуса любой документированной информации включается в нарушении ее физической сохранности (вообще либо у данного собственника в полном или частичном объеме), логической структуры и содержания, доступности для правомочных пользователей. Нарушение статуса конфиденциальной документированной информации дополнительно включает нарушение ее конфиденциальности (закрытости для посторонних лиц).

Уязвимость документированной информации – понятие собирательное. Она не существует вообще, а проявляется в различных формах. К таким формам, выражающим результаты дестабилизирующего воздействия на информацию, относятся (в скобках указаны существующие варианты названий форм):

– хищение носителя информации или отображенной в нем информации (кража);

– потеря носителя информации (утеря);

– несанкционированное уничтожение носителя информации или отображенной в нем информации (разрушение);

– искажение информации (несанкционированное изменение, несанкционированная модификация, подделка, фальсификация);

– блокирование информации;

– разглашение информации (распространение, раскрытие).

Термин «разрушение» употребляется главным образом применительно к информации на машинных носителях.

Существующие варианты названий: модификация, подделка, фальсификация – не совсем адекватны термину «искажение», они имеют нюансы, однако суть их одна и та же – несанкционированное частичное и полное изменение состава первоначальной информации.

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

Разглашение информации является формой проявления уязвимости только конфиденциальной информации.

Та или иная форма уязвимости документированной информации может реализоваться в результате преднамеренного или случайного дестабилизирующего воздействия различными способами на носитель информации или на саму информацию со стороны источников воздействий. Такими источниками могут быть люди, технические средства обработки передачи информации, средства связи, стихийные бедствия и др. Способами дестабилизирующего воз-

действия на информацию являются копирование (фотографирование), записывание, передача, съем, заражение программ обработки информации вирусом, нарушение технологии обработки и хранения информации, вывод (или выход) из строя и нарушение режима работы технических средств обработки и передачи информации, физическое воздействие на информацию и др.

Реализация форм проявления уязвимости документированной информации приводит или может привести к двум видам уязвимости:

– утрате информации;

– утечке информации.

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

К утечке конфиденциальной документированной информации приводит ее разглашение. В литературе и даже в нормативных документах термин «утечка конфиденциальной информации» нередко заменяется или отождествляется с терминами; «разглашение конфиденциальной информации», «распространение конфиденциальной информации». Такой подход не является правомерным.

Разглашение или распространение конфиденциальной информации означают несанкционированное доведение ее до потребителей, не имеющих права доступа к ней. При этом такое доведение должно осуществляться кем-то, исходить от кого-то. Утечка происходит при разглашении (несанкционированном распространении) конфиденциальной информации, но не сводится только к нему. Утечка может произойти и в результате потери носителя конфиденциальной документированной информации, а также хищения носителя информации либо отображенной в нем информации при сохранности носителя у его собственника (владельца). «Может произойти» не означает, что произойдет. Потерянный носитель может попасть в чужие руки, а может быть и «прихвачен» мусороуборочной машиной и уничтожен в установленном для мусора порядке. В последнем случае утечки конфиденциальной информации не происходит.

Хищение конфиденциальной документированной информации также не всегда связано с получением ее лицами, не имеющими к ней доступа. Имелось немало случаев, когда хищение носителей конфиденциальной информации осуществлялось у коллег по работе допущенными к этой информации лицами с целью «подсидки», причинения вреда коллеге. Такие носители, как правило, уничтожались лицами, похитившими их.

Но в любом случае потеря и хищение конфиденциальной информации если и не приводят к ее утечке, то всегда создают угрозу утечки. Поэтому можно сказать, что к утечке конфиденциальной информации приводит ее разглашение, и могут привести хищение и потеря. Сложность состоит в том, что зачастую невозможно определить, во-первых, сам факт разглашения или хищения конфиденциальности информации при сохранности носителя информации у ее собственника (владельца), во-вторых, попала ли информация вследствие ее хищения или потери посторонним лицам.

Суммируя соотношение форм и видов уязвимости защищаемой информации, можно констатировать:

1. Формы проявления уязвимости информации выражают результаты дестабилизирующего, воздействия на информацию, а виды уязвимости – конечный суммарный итог реализации форм проявления уязвимости.

2. Утрата информации включает в себя, по сравнению с утечкой, большее число форм проявления уязвимости информации, но она не поглощает утечку, т. к. не все формы прояв-

ления уязвимости информации, которые приводят или могут привести к утечке, совпадают с формами, приводящими к утрате.

3. Наиболее опасными формами проявления уязвимости конфиденциальной документированной информации являются потеря, хищение и разглашение – первые две одновременно могут привести и к утрате, и к утечке информации, вторая (хищение информации при сохранности носителя) и третья могут не обнаружиться, со всеми вытекающими из этого последствиями.

4. Неправомерно отождествлять, как это нередко делается в научной литературе и нормативных документах, включая законы, виды и отдельные формы проявления уязвимости информации (утрата = потеря, утрата = хищение, утечка = разглашение (распространение)), а также формы проявления уязвимости информации и способы дестабилизирующего воздействия на нее.

5. Необходимо уделять одинаковое внимание предотвращению как утраты защищаемой документированной информации, так и ее утечки, т. к. ущерб собственнику информации наносится в любом случае.

Защита конфиденциальной документированной информации от утраты и утечки осуществляется в определенной мере в рамках и первой, второй составляющих конфиденциального делопроизводства, т. к. она взаимоувязана, «переплетена» с ними: документирование конфиденциальной информации и организация работы с конфиденциальными документами должны производиться в условиях обеспечения их защиты, и вместе с тем многие вопросы защиты решаются в ходе и путем осуществления систематических операций по учету и обработке документов. Однако защитные мероприятия охватывают не только сами документы, но и другие объекты, так или иначе связанные с защищаемыми документами (помещения, технические средства обработки и передачи информации и др.)

Поэтому в определении конфиденциального делопроизводства защита документированной информации выделена в самостоятельную составляющую.

Конфиденциальное делопроизводство шире открытого и по своим задачам. Если задачей открытого делопроизводства является документационное обеспечение управленческой деятельности, то конфиденциальное делопроизводство должно осуществлять решение двух задач:

1) документационное обеспечение всех видов конфиденциальной деятельности;

2) защита документированной информации, образующейся в процессе конфиденциальной деятельности.

Первая задача имеет своей целью организацию и бесперебойное функционирование конфиденциальной деятельности в сфере любого вида производства и управления. Это требует от делопроизводства обеспечения нужд конфиденциальной деятельности полной, своевременной и достоверной документной информацией, организации исполнения и использования документов.

Полноту документной 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, не нужной для деятельности предприятия информации.

Достоверность документной информации заключается, во-первых, в ее соответствии объективному состоянию того или другого вопроса и, во-вторых, в ее юридической силе, характеризующейся наличием и правильностью оформления соответствующих реквизитов.

Своевременность документной 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 своевременного и качественного решения содержащихся в документах вопросов.

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

Вторая задача имеет своей целью обеспечение сохранности и конфиденциальности документированной информации, что требует создания и поддержания специальных условий хранения, обработки и обращения документов, гарантирующих надежную защиту, как самих документов, так и содержащейся в них информации. Сущность конфиденциального делопроизводства обусловливает его организационные и технологические особенности, к числу основных из которых относятся:

– письменное нормативное закрепление общей технологии документирования, организации работы с документами и их защиты;

– жесткое регламентирование состава издаваемых документов и содержащейся в них информации, в том числе на стадии подготовки черновиков и 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, к ее защите;

– персональная и обязательная ответственность за учет, сохранность документов и порядок обращения с ними.

Особенностью конфиденциального делопроизводства является и своеобразное переплетение некоторых функций, которые на первый взгляд как бы взаимоисключают друг друга. В частности, функциями по реализации задачи документационного обеспечения конфиденциальной деятельности являются создание документов, необходимых и достаточных для такой деятельности, предоставление каждому пользователю всех документов, требующихся для выполнения должностных обязанностей, параллельными им функциями по реализации задачи защиты конфиденциальной информации – предотвращение необоснованного издания и рассылки документов, исключение необоснованного ознакомления с документами.

На самом деле применительно к документированию это означает, что конфиденциальная деятельность должна обеспечиваться минимальным количеством документов при сохранении полноты и достоверности информации, применительно к организации документооборота – предоставление пользователям всех необходимых документов, но только тех, которые действительно требуются для выполнения должностных обязанностей.

Особенности конфиденциального делопроизводства одновременно выступают и в качестве требований к нему.

Лекция 2. Меры по обеспечению защиты коммерческой тайны

Меры по обеспечению защиты коммерческой тайны условно можно классифицировать на внутренние и внешние, которые в свою очередь делятся на правовые, организационные, технические и психологические. Некоторые источники выделяют еще одну – страховую, т. е. страхование коммерческой тайны от ее разглашения. Однако в наших условиях такой метод защиты представляется нам малореальным. Кроме того, очень тяжело определить реальную стоимость принадлежащей предприятию коммерческой тайны. Меры по обеспечению защиты коммерческой тайны предприятия показаны на рисунке 1.

Рис. 1

Действие внутренних мер по обеспечению конфиденциальности в основном направлено на рабочий персонал вашего предприятия. Работники хозяйствующего субъекта, имеющие доступ к сведениям, составляющим коммерческую тайну, обязуются:

– сохранять коммерческую тайну, которая станет им известна по работе, и не разглашать ее без разрешения, выданного в установленном порядке, при условии, что сведения, составляющие коммерческую тайну, не были известны им ранее либо не были получены ими от третьего лица без обязательства соблюдать в отношении их конфиденциальность;

– выполнять требования инструкций, положений, приказов по обеспечению сохранности коммерческой тайны;

– в случае попытки посторонних лиц получить от них сведения, составляющие коммерческую тайну, немедленно сообщить об этом соответствующему должностному лицу или в соответствующее подразделение хозяйствующего субъекта;

– сохранять коммерческую тайну хозяйствующих субъектов, с которыми имеются деловые отношения;

– не использовать знание коммерческой тайны для занятий деятельностью, которая в качестве конкурентного действия может нанести ущерб хозяйствующему субъекту;

– в случае увольнения передать все носители информации, составляющие коммерческую тайну (рукописи, черновики, документы, чертежи, диски, «флешки», дискеты, распечатки на принтерах, кино-, фотопленки, модели, материалы и др.), которые находились в их распоряжении, соответствующему должностному лицу или в соответствующее подразделение хозяйствующего субъекта.

Данные обязательства даются в письменной форме при заключении трудового или иного договора либо в процессе его исполнения.

Внешние меры по обеспечению конфиденциальности коммерческой тайны необходимы при осуществлении вами торгово-экономических, научно-технических, валютно-финансовых и других деловых связей, в том числе с иностранными партнерами. Для этого договаривающиеся стороны специально оговаривают характер, состав сведений, составляющих коммерческую тайну, а так же взаимные обязательства по обеспечению её сохранности в соответствии с законодательством. Однако нужно помнить, что при заключении договора с иностранными партнерами условия конфиденциальности деятельности должны соответствовать законодательству страны, где заключается договор, если иное не предусмотрено межгосударственными соглашениями. В данном случае применяется принцип, сформулированный еще в римском праве – «locus regit actum».

Locus regit actum (место руководит актом) – начало частного международного права, в силу которого внешние формы и обряды совершения актов (договоров, завещаний, браков) определяются законами факультативно того места, где они совершены.

Правовые меры обеспечения сохранности коммерческой тайны являются первоочередными, т. к. они призваны обеспечить эффективное функционирование остальных мер обеспечения конфиденциальности информации. С этой точки зрения правовые меры являются первичными по отношению к остальным мерам.

Первым шагом по реализации правовых мер является принятие на предприятии Положения (Инструкции) по обеспечению сохранности коммерческой тайны, в которых определяются:

– состав и объем сведений, составляющих коммерческую тайну;

– порядок присвоения грифа «Секрет предприятия» сведениям, работам и изделиям и его снятия;

– процедура допуска работников хозяйствующего субъекта, а также лиц, привлекаемых к его деятельности, к сведениям, составляющим коммерческую тайну;

– порядок использования, учета, хранения и маркировки документов и иных носителей информации, изделий, сведения о которых составляют коммерческую тайну;

– организация контроля за порядком использования сведений, составляющих коммерческую тайну;

– процедура принятия взаимных обязательств хозяйствующими субъектами по сохранению коммерческой тайны при заключении договоров о проведении каких-либо совместных действий;

– порядок применения предусмотренных законодательством мер дисциплинарного и материального воздействия на работников, разгласивших коммерческую тайну;

– возложение ответственности за обеспечение сохранности коммерческой тайны на должностное лицо хозяйствующего субъекта.

После принятия Положения можно приступать к разработке организационных мер обеспечения конфиденциальности вашей коммерческой тайны.

Одним из наиболее важнейших вопросов, требующих разрешения является вопрос, кто будет осуществлять все перечисленные меры по защите. Естественно, исполнение этих обязанностей должно быть поручено специалистам, обладающим необходимыми теоретическими и практическими знаниями. Не рекомендуется использование для этих целей услуг частных охранных и детективных агентств, так как: во-первых, перед ними стоят несколько иные задачи (физическая охрана и техническая безопасность объекта), а, во-вторых, вряд ли здравомыслящий бизнесмен разрешит доступ к своей коммерческой тайне посторонним лицам, пусть даже представляющим охранное агентство.

Для обеспечения защиты коммерческой тайны на крупных хозяйствующих объектах могут создаваться специальные режимно-секретные подразделения, функции, полномочия которых отражаются в соответствующих инструкциях, положениях, приказах.

Такие подразделения должны быть созданы не только на крупных объектах, но и на всех остальных, занимающихся коммерческой деятельностью. На любом предприятии имеются сведения, подлежащие защите, разница только в объеме мер защиты. Если на крупных хозяйствующих объектах, таких как банки, финансовые корпорации, заводы, специализированное подразделение представлено в виде разветвленной, отлично материально и технически оснащенной структуры, в которой может работать несколько десятков сотрудников, то на средних и малых предприятиях такое подразделение может быть представлено в виде нескольких ответственных сотрудников. В крайнем случае, если предприятие не может себе позволить содержать таких сотрудников в своем штате, то следует прибегнуть к услугам консультантов по вопросам безопасности и защиты информации. Они помогут разработать необходимую систему защиты, а также решить возникающие в ходе практической деятельности вопросы.

Лекция 3. Организация конфиденциального делопроизводства

Организация конфиденциального делопроизводства означает создание необходимых условий для изготовления и получения конфиденциальных документов, организации работы с ними и предотвращения утраты и утечки документированной конфиденциальной информации.

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, выделение для подразделения служебного помещения, обеспечение необходимых условий труда, разработку или приобретение нормативных документов и методической литературы по организации и ведению конфиденциального делопроизводства, создание постоянно действующей экспертной комиссии, оформление допуска сотрудников к коммерческой и служебной тайне и обучение их правилам работы с конфиденциальными документами.

Конфиденциальное делопроизводство в силу небольшого по сравнению с открытым делопроизводством объема документов и в целях обеспечения условий для сохранности и конфиденциальности документов должно быть централизованным, т. е. сосредоточенным в едином подразделении предприятия. Подразделение конфиденциального делопроизводства может быть самостоятельным структурным подразделением предприятия, подчиненным непосредственно руководителю предприятия, или входить в состав других подразделений, как правило, осуществляющих защиту конфиденциальной информации: службу безопасности, службу защиты информации и др. В «Положении о порядке обращения со служебной информацией ограниченного распространения» сказано: «Прием и учет (регистрация) документов, содержащих служебную информацию ограниченного распространения, осуществляются, как правило, структурными подразделениями, которым поручен прием и учет несекретной документации», однако это целесообразно лишь при незначительном объеме таких документов и при отсутствии документов, содержащих коммерческую тайну.

Наименование подразделения конфиденциального делопроизводства, статус и при необходимости структуру определяет руководитель предприятия, исходя из объема конфиденциального делопроизводства и общей структуры предприятия.

Подразделение конфиденциального делопроизводства является составной частью системы защиты коммерческой и служебной тайны, органом, осуществляющим, координирующим и контролирующим работу с конфиденциальными документами. Оно должно рассматриваться как структурное подразделение, непосредственно участвующее в основной деятельности предприятия. Численный состав сотрудников подразделения конфиденциального делопроизводства должен определяться объемом выполняемой работы с учетом норм времени на ее выполнение.

Должностной состав сотрудников подразделения конфиденциального делопроизводства должен определяться характером и сложностью выполняемой работы. Для более многообразной и более сложной работы следует устанавливать и более высокие должности.

При незначительном объеме конфиденциального делопроизводства специальное подразделение конфиденциального делопроизводства может не создаваться. В этом случае издание, обработка и хранение конфиденциальных документов возлагается на специально назначенных приказом руководителя предприятия нескольких либо одного сотрудников других подразделений, как правило, службы безопасности или, как было сказано, службы открытого делопроиз-

водства, если документы содержат сведения, составляющие только служебную тайну. На этих лиц распространяются все задачи, функции, права и ответственность, возлагаемые на подразделение конфиденциального делопроизводства.

Если ведение конфиденциального делопроизводства возложено на одного сотрудника, то для выполнения отдельных делопроизводственных операций, в которых требуется участие двух лиц (проверки наличия, уничтожение документов), необходимо привлекать (лучше на постоянной основе) второго сотрудника данного или другого подразделения, имеющего доступ к этим документам. Такое привлечение оформляется приказом по предприятию. 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 печатанию, учету, размножению, хранению, передаче, отправлению, систематизации, проверке наличия и уничтожению конфиденциальных документов. Функции исполнителей и пользователей конфиденциальных документов в сфере изготовления и обработки документов ограничиваются подготовкой документов и их исполнением. Допустимо и печатание документов исполнителями, если оно осуществляется в специально предназначенном для этого помещении подразделения конфиденциального делопроизводства.

Основные задачи и функции подразделения конфиденциального делопроизводства, а также права и ответственность его руководителя должны быть закреплены в положении о подразделении, а обязанности, права, ответственность сотрудников подразделения конфиденциального делопроизводства или специально назначенных для ведения конфиденциального делопроизводства лиц – в должностных инструкциях, разрабатываемых на конкретные должности. В должностных инструкциях устанавливаются и квалификационные требования к сотрудникам – образование и стаж работы на аналогичной должности. 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 предприятия, но и участвовать во всех мероприятиях по предотвращению утраты конфиденциальных документов и утечки содержащейся в них информации. Это участие не ограничивается разработкой и осуществлением соответствующих мероприятий только в рамках подразделения конфиденциального делопроизводства. Утрата и утечка конфиденциальной информации в большинстве случаев происходят по вине исполнителей 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 прав работы с конфиденциальными документами и осуществлением контроля за их выполнением. Этим обусловлены и соответствующие права подразделения конфиденциального делопроизводства, в том числе такие, участие в подборе кадров для работы с конфиденциальной информацией, внесение предложений об отстранении от конфиденциальных работ, поощрении и привлечении к ответственности исполнителей и пользователей конфиденциальных документов, участие в проведении расследований по фактам утраты и утечки конфиденциальной информации.

При разработке должностных инструкций следует учитывать, во-первых, необходимость специализации сотрудников по отдельным видам работ, что ускоряет их выполнение и повышает качество, и, во-вторых, нормативы времени на работы с тем, чтобы все сотрудники были загружены равномерно в соответствии с должностью, и не было перезагруженности, которая отрицательно сказывается на качестве работы. При установлении квалификационных требо-

ваний к должностям необходимо иметь в виду сложность выполнения некоторых видов работ, требующих специальной подготовки. На соответствующие таким работам должности следует назначать специалистов с высшим образованием в области защиты информации. В соответствии с законодательством сотрудники подразделения конфиденциального делопроизводства несут дисциплинарную, административную либо гражданско-правовую ответственность за утрату конфиденциальных документов или разглашение содержащейся в них информации, поэтому в должностных инструкциях должна быть установлена персональная ответственность сотрудников за сохранность конфиденциальных документов и содержащейся в них информации. В случаях особой конфиденциальности документов назначение сотрудников на соответствующие должности в подразделение конфиденциального делопроизводства целесообразно осуществлять после проведения в отношении их полномочными органами проверочных мероприятий при письменном согласии на это сотрудников.

Конец ознакомительного фрагмента.