



## ПРИКАЗ

01 ноября 2022

№ 01.11.2

*О Положении О сведениях  
конфиденциального характера*

### ПРИКАЗЫВАЮ:

1. Ввести в действие с 01.11.2022 года Положение *О сведениях конфиденциального характера* в новой редакции, утвержденной настоящим Приказом.
2. Положение *О сведениях конфиденциального характера*, утвержденного приказом от 27.12.2019 № 27.12.9, считать утратившим силу с 01.11.2022 года.
3. С приказом ознакомить всех руководителей подразделений.
4. Контроль исполнения приказа оставляю за собой.

Генеральный директор

М.Е.Козлов

**ПОЛОЖЕНИЕ  
О СВЕДЕНИЯХ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА  
ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ  
"ВЫСОТКА"**

г. МОСКВА  
2022

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Положение разработано в соответствии с Гражданским кодексом Российской Федерации, Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».

1.2. Положение устанавливает порядок обращения со сведениями конфиденциального характера, являющимися собственностью Общества с ограниченной ответственностью "ВЫСОТКА" (далее - Общество), его контрагентов и определяет основные меры их защиты с целью предотвращения нанесения ущерба экономической безопасности Общества вследствие неправомерного использования таких сведений – их утраты, хищения, разглашения или фальсификации.

1.3. Цель Положения - определение основных мер защиты сведений конфиденциального характера, установление порядка обращения со данными сведениями с целью предотвращения возможного нанесения ущерба экономической безопасности Общества вследствие неправомерного использования данных сведений (их утраты, хищения, разглашения или фальсификации).

1.4. Положение является основополагающим нормативным документом, регламентирующим деятельность Общества в сфере защиты сведений конфиденциального характера. Требования Положения обязательны для выполнения всеми работниками Общества.

1.5. Действие настоящего Положения не распространяется на устанавливаемый государственными органами режим защиты сведений, составляющих государственную тайну Российской Федерации.

1.6. Руководители структурных подразделений Общества несут персональную ответственность за обеспечение охраны сведений конфиденциального характера на участке деятельности подразделения, организуют выполнение установленных Положением режимных требований, принимают меры по максимальному ограничению возможности ознакомления с информацией работников, которым по роду выполняемых ими должностных обязанностей она не требуется.

1.7. В вопросах сохранения сведений конфиденциального характера, предоставляемых Обществу контрагентами, следует руководствоваться действующим законодательством Российской Федерации, Положением, а также условиями обеспечения охраны данных сведений, изложенными в соответствующих договорах и (или) соглашениях, заключенных с контрагентами.

1.8. Все структурные подразделения и работники Общества; контрагенты, допускаемые к сведениям конфиденциального характера; лица, оказывающие Обществу услуги в соответствии с заключенными договорами возмездного оказания услуг, если эти услуги связаны с доступом к сведениям конфиденциального характера - являются пользователями Положения.

1.9. Права на настоящее Положение принадлежат Обществу. Настоящее Положение не может быть полностью или частично воспроизведено, опубликовано, тиражировано, скопировано или распространено в любой иной форме без разрешения Общества.

## 2. НОРМАТИВНЫЕ ССЫЛКИ

- 2.1. В Положении использованы ссылки на следующие нормативные документы:
1. Статьи 23, 24 Конституции Российской Федерации.
  2. Глава 75 Гражданского кодекса Российской Федерации.
  3. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
  4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
  5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
  6. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».
  7. Постановление Правительства РСФСР от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

## 3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Исполнитель** – сотрудник иницирующего составление документа (в том числе, заключение Договора, Контракта и пр.) подразделения Общества, являющийся ответственным за прохождение и исполнение документа в соответствии с требованиями локальных нормативных актов Общества.

**Информация** - сведения (сообщения, данные), независимо от формы их представления.

**Обладатель информации** – лицо, которое владеет информацией на законном основании, ограничило к ней доступ и установило в отношении ее соответствующий режим защиты.

**Обработка информации** - получение, хранение, преобразование, комбинирование, передача или любое другое использование информации.

**Защита информации** - организационные, правовые, технические и технологические меры по предотвращению угроз информационной безопасности и устранению их последствий.

**Средства защиты информации** - технические, криптографические, программные и другие средства, предназначенные для защиты сведений конфиденциального характера, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

**Разглашение информации** – несанкционированное доведение в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) сведений конфиденциального характера до третьих лиц, не имеющих права доступа к этим сведениям.

**Носители информации** - материальные объекты, в том числе физические поля, в которых сведения конфиденциального характера находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

**Машинный носитель информации** - материальный носитель или устройство, предназначенное для записи, хранения и считывания сведений конфиденциального характера средствами вычислительной и (или) оргтехники - персональными компьютерами (рабочими станциями), серверами и другими техническими средствами.

**Энергонезависимый машинный носитель информации** - машинный носитель информации, сведения конфиденциального характера в которых, в отличие от энергозависимых машинных носителей информации, сохраняется после отключения электропитания или их изъятия из устройств, в которые они устанавливаются.

**Документ (документированная информация)** - зафиксированная на материальном носителе информация с реквизитами, позволяющими идентифицировать информацию или ее материальный носитель.

**Документ на машинном носителе (электронный документ)** - документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

**Утрата документов** - выход (в том числе и временный) документов из владения ответственного за их сохранность работника, которому они были доверены, вследствие чего эти документы, а равно содержащиеся в них сведения, стали, либо могли стать достоянием посторонних лиц.

**Гриф ограничения доступа к документу** (ограничительный гриф) - реквизит официального документа, свидетельствующий об особом характере информации, ограничивающий круг пользователей документом.

**Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Информационная безопасность** - состояние защищенности информационной среды Общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

**Доступ к сведениям конфиденциального характера** - ознакомление определенных лиц со сведениями конфиденциального характера, с согласия их обладателя или на ином законном основании при условии сохранения конфиденциальности этих сведений.

**Передача сведений конфиденциального характера** - передача сведений конфиденциального характера, зафиксированных на материальном носителе, их обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране их конфиденциальности.

**Предоставление сведений конфиденциального характера** - передача сведений конфиденциального характера и зафиксированных на материальном носителе, их обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Лица, виновные в разглашении сведений конфиденциального характера, а также допустившие нарушение порядка обращения с документами, содержащими сведения конфиденциального характера, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

**Контрагент** - сторона гражданско-правового договора, которой обладатель сведений конфиденциального характера передал эти сведения.

**Контрагент Общества** - юридические и физические лица, с которыми взаимодействует Общество при выполнении работ (оказании услуг) на основании заключенных договоров (соглашений, контрактов).

**Сведения конфиденциального характера** - требующая защиты документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Сведения конфиденциального характера состоят из:

1. **коммерческой тайны** - сведений любого характера (производственные, технические, экономические, организационные, о результатах интеллектуальной деятельности в научно-технической сфере, о способах осуществления профессиональной деятельности), связанных с коммерческой деятельностью Общества, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам вследствие отсутствия свободного доступа к ним, в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Перечень сведений, составляющих коммерческую тайну, утверждается Обществом и является неотъемлемой частью настоящего Положения (Приложение 1).

Разглашение (утечка) данных сведений может привести к подрыву экономической безопасности Общества в целом, лишить его занимаемого положения на рынке, существенно снизить прибыль, сорвать реализацию стратегических планов, вызвать осложнения на отдельных направлениях деятельности Общества, а также может снизить эффективность работы с контрагентами и клиентами, создать физическую угрозу безопасности объектов, имуществу и персоналу, привести к дополнительным материальным затратам.

Режим коммерческой тайны - правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.

Документированным сведениям, отнесенным к указанной категории, присваивается ограничительный гриф «Коммерческая тайна» («КТ»).

На материальных носителях с указанными документированными сведениями проставляется наименование их обладателя и его местоположение.

Не является коммерческой тайной информация, которая в соответствии с действующим законодательством РФ не может быть отнесена к коммерческой тайне, а также информация, разглашенная Обществом или работником в порядке, установленном настоящим Положением.

**2. сведений конфиденциального характера, не являющихся коммерческой тайной** – сведений, которые не могут быть отнесены к коммерческой тайне, но не должны быть общедоступными, так как предание их огласке нанесет ущерб интересам Общества, его контрагентов и/или персонала, ограничения к доступу и разглашению которых предпринимаются Обществом в соответствии с действующим законодательством РФ, и внутренними актами Общества, в том числе, настоящим Положением. К Сведениям конфиденциального характера, не являющимися коммерческой тайной, в том числе, относятся:

2.1. информация служебного характера, которая не может быть отнесена к коммерческой тайне согласно требованиям законодательства:

- статистические и отчетные документы, форма и содержание которых установлены нормативными актами органов государственной власти;
- платежные документы;
- сведения об исчислении и уплате налогов и обязательных платежей, о численности и составе работающих, их заработной плате и др.;

2.2. служебная тайна - информация, ограничения на распространение которой (режим служебной тайны) диктуются действующим законодательством РФ и служебной необходимостью. Перечень сведений, составляющих служебную тайну, утверждается Обществом и является неотъемлемой частью настоящего Положения (Приложение 1).

Не является служебной тайной информация, которая в соответствии с действующим законодательством РФ не может быть отнесена к служебной тайне, а также информация, разглашенная Обществом или работником в порядке, установленном настоящим Положением.

На документах, содержащих сведения, определенные Перечнем сведений, составляющих служебную тайну Общества, проставляется гриф "ДСП" - Для служебного пользования.

Лица, виновные в разглашении служебной тайны, а также допустившие нарушение порядка обращения с документами, содержащими такую информацию, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

2.3. сведения, защищаемые государством в иных режимах:

- 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 так далее);

- сведения, составляющие тайну следствия и судопроизводства;

- сведения, защищаемые нормами патентного, авторско-правового и иного специального законодательства;

- персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Перечень сведений, составляющих персональные данные работников Общества, а также порядок их получения, обработки и хранения, определяется Положением об обработке и защите персональных данных в ООО «ВЫСОТКА».

2.4. сведения, доступ к которым ограничен органами государственной власти.

На документах, указанных в пп. 2.1 и документах, конфиденциальность которых определена законом и порядок учета, хранения и обращения с которыми определяется специальными нормами законодательства, ограничительный гриф "Конфиденциально" («К») не проставляется.

Поступающие из государственных структур документы, содержащие служебную тайну, с проставленным на них ограничительным грифом "Для служебного пользования" (ДСП),

являются конфиденциальными по своему статусу, и на них распространяется режим защиты, установленный настоящим Положением для конфиденциальных материалов.

Документооборот материалов с ограничительным грифом "Конфиденциально", а равно и с пометкой "Для служебного пользования", осуществляется в системе общего делопроизводства с соблюдением требований внутренних актов Общества и настоящего Положения.

Документированным сведениям, отнесенным к указанной категории (за вышеуказанными исключениями), присваивается ограничительный гриф «Конфиденциально».

На материальных носителях с указанными документированными сведениями наименование их обладателя и его местоположение не проставляется.

#### 4. СОКРАЩЕНИЯ

В настоящем Положении применены следующие сокращения:

| Сокращение | Наименование сокращения  |
|------------|--|
| Общество   | Общество с ограниченной ответственностью "ВЫСОТКА"   |
| КТ         | Гриф "Коммерческая тайна"  |
| К          | Гриф "Конфиденциально"   |
| ДСП        | Гриф "Для служебного пользования"  |
| СВТ        | Средства вычислительной техники  |
| Перечень   | Перечень сведений, составляющих коммерческую тайну ООО "ВЫСОТКА", и иных конфиденциальных сведений |
| Положение  | Положение о коммерческой тайне ООО "ВЫСОТКА"   |

#### 5. ПОРЯДОК ОТНЕСЕНИЯ СВЕДЕНИЙ К СВЕДЕНИЯМ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, СНЯТИЯ ОГРАНИЧЕНИЙ НА РАСПРОСТРАНЕНИЕ СВЕДЕНИЙ

5.1. В соответствии с Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» к сведениям конфиденциального характера относятся:

а) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

б) служебные сведения, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

в) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

г) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них;

д) 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 так далее);

е) сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20.08.2004 № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными

правовыми актами Российской Федерации.

5.2. Отнесение сведений к сведениям конфиденциального характера производится:

а) в отношении информации, исключительным собственником которой является Общество, в соответствии с Перечнем сведений конфиденциального характера (далее - Перечень);

б) в отношении сведений конфиденциального характера, собственниками которых являются другие юридические и физические лица, - в соответствии с договорами и (или) соглашениями с правообладателями этих сведений конфиденциального характера.

5.3. Перечень утверждается приказом Генерального директора и доводится до работников Общества при приеме их на работу и при внесении изменений в настоящее Положение.

Перечень подлежит пересмотру один раз в три года, а также в иных случаях по решению Генерального директора Общества.

5.4. Согласно ст. 5 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне» режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

а) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

б) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

в) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

г) 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;

д) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости и о наличии свободных рабочих мест;

е) о задолженности работодателей по выплате заработной платы и социальным выплатам;

ж) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

з) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

и) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

к) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

л) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

5.5. Персональную ответственность за правильность определения степени конфиденциальности и своевременность проставления ограничительных грифов на документах и иных материальных носителях несет Исполнитель, а также лицо, подписывающее (утверждающее) документ.

Проставление ограничительных грифов на документах производит **Начальник Юридической службы Общества** после получения по электронной почте письменного согласования от непосредственного руководителя Исполнителя.

В случае отсутствия на документе любого из упомянутого в настоящем Положении грифа – данный документ не является документом конфиденциального характера.

5.6. Если сведения не предусмотрены Перечнем, но, по мнению Исполнителя, должны быть отнесены к сведениям конфиденциального характера, он представляет согласованные с руководителем подразделения аргументированные предложения в Юридическую службу о

внесении соответствующих дополнений в Перечень. До принятия решения защита указанных сведений должна быть обеспечена в соответствии с требованиями Положения.

Этот порядок применяется и в случае признания необходимости снижения ограничительного грифа или исключения из Перечня тех или иных сведений.

5.7. Сведения конфиденциального характера утрачивают необходимость защиты:

- а) по исключению из Перечня;
- б) по соглашению заинтересованных сторон, установивших ограничения;
- в) в случае принятия решения руководством Общества об открытом оглашении сведений и после фактически состоявшегося оглашения;
- г) в иных случаях, определяемых лицом, утвердившим Перечень.

5.8. Снятие ограничений на распространение сведений конфиденциального характера производится по решению Генерального директора Общества на основании обоснованного представления структурного подразделения, являющегося владельцем сведений.

5.9. Снятие ограничений на распространение сведений конфиденциального характера, которые являются результатом совместной деятельности Общества и других юридических и физических лиц, допускается только по согласованию с ними.

5.10. О снятии ограничений на распространение сведений конфиденциального характера извещаются юридические и физические лица, которым эти сведения были переданы на договорных условиях.

## **6. ОХРАНА СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА**

6.1. Общество имеет исключительное право на использование и обработку сведений конфиденциального характера в экономической деятельности, включая их использование в деятельности по организации и проведению выставок, ярмарок, салонов и других выставочных мероприятий, передачу другим лицам на основании договоров, а также иные способы включения указанных сведений в хозяйственный оборот в порядке, установленном действующим законодательством РФ, внутренними актами Общества, в том числе, настоящим Положением.

6.2. Охрана сведений конфиденциального характера осуществляется в целях обеспечения экономической, правовой и организационной безопасности Общества, обеспечения прав и свобод человека и гражданина.

Охрана сведений конфиденциального характера заключается в принятии Обществом комплекса организационных и технических мер, направленных:

- на ограничение доступа третьих лиц к сведениям конфиденциального характера;
- на предотвращение несанкционированного разглашения сведений конфиденциального характера;
- на выявление и пресечение нарушений порядка обращения с документами, содержащими сведения конфиденциального характера;
- на привлечение лиц, виновных в разглашении сведений конфиденциального характера, а также допустивших нарушение порядка обращения с документами, содержащими такие сведения, к дисциплинарной, административной, гражданско-правовой или уголовной ответственности в соответствии с действующим законодательством и настоящим Положением.

6.3. Общество обеспечивает доступ к сведениям конфиденциального характера работникам и третьим лицам в случаях и порядке, предусмотренных действующим законодательством РФ и настоящим Положением.

6.4. Режим охраны сведений конфиденциального характера в Обществе устанавливается в отношении сведений конфиденциального характера, обладателем которых являются Общество, другие юридические и физические лица, если в заключенных с ними договорах (соглашениях) оговорена необходимость обеспечения охраны конфиденциальности таких сведений.

6.5. Режим охраны сведений конфиденциального характера устанавливается:

- а) в отношении сведений, исключительным собственником которых является Общество в соответствии с Положением, и разработанных на его основе других внутренних нормативных документов;



б) в отношении сведений, собственниками которых являются другие юридические и физические лица, - в соответствии с договорами и (или) соглашениями с правообладателями этой информации;

в) в отношении персональных данных работников Общества, командированных лиц и посетителей - в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и в соответствии с Положением об обработке и защите персональных данных в ООО «ВЫСОТКА»;

г) в отношении иных сведений ограниченного доступа - в соответствии с требованиями действующего законодательства Российской Федерации, указами Президента Российской Федерации, постановлениями Правительства Российской Федерации или уполномоченных ими компетентных органов.

6.6. Сведения конфиденциального характера предоставляются только тем работникам, которым доступ к таким сведениям необходим в силу выполнения ими трудовых обязанностей, в объеме и порядке, исключающих их несанкционированное разглашение.

Работники, допущенные к сведениям конфиденциального характера, прежде чем получить доступ к ним, должны пройти инструктаж и ознакомиться с Памяткой работнику о сохранении сведений конфиденциального характера (Приложение 3).

6.7. Обязательным условием трудовых договоров, заключаемых Обществом с работниками, является условие о неразглашении сведений конфиденциального характера.

6.8. Обязательными мерами по обеспечению защиты сведений конфиденциального характера является включение в гражданско-правовые договоры обязательства сторон о неразглашении сведений конфиденциального характера.

6.9. Сведения конфиденциального характера, затрагивающие права, свободы и законные интересы конкретного работника, могут быть предоставлены ему лично, его уполномоченному представителю или с письменного согласия работника третьему лицу.

6.10. В служебных и архивных помещениях Общества создаются условия, ограничивающие доступ третьих лиц к сведениям конфиденциального характера и несанкционированное разглашение конфиденциальных сведений, в том числе устанавливаются технические средства защиты от несанкционированного доступа к информации (сейфы и металлические ящики для хранения документов и пр.).

6.11. Организация охраны сведений конфиденциального характера возлагается на назначаемого соответствующим приказом сотрудника **Административного департамента Общества.**

## **7. РАБОТА С ДОКУМЕНТАМИ, СОДЕРЖАЩИМИ СВЕДЕНИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА**

7.1. Для всех структурных подразделений Общества устанавливается единый порядок учета, хранения, размножения, рассылки и уничтожения документальных материалов, содержащих сведения конфиденциального характера.

7.2. Документы с грифами "КТ", "К", "ДСП" или "ПД", образующиеся в деятельности Общества, в обязательном порядке должны содержать на обороте последнего листа каждого экземпляра документа информацию о конкретном Исполнителе и дате создания документа. Черновики и предварительные варианты документа уничтожаются непосредственным Исполнителем документа после его подписания и вступления в силу.

7.3. Подготовленные и подписанные документы:

- передаются работникам подразделений под роспись в соответствии с листом рассылки;
- пересылаются сторонним организациям заказными или ценными почтовыми отправлениями;

- копируются (тиражируются) только с письменного разрешения соответствующего руководителя;

- хранятся в запираемых шкафах (ящиках, сейфах) в служебных или архивных помещениях, ключи от которых сдаются на пост Отдела внутреннего мониторинга.

Передача документов и дел с грифами "КТ", "К", "ДСП" или "ПД" от одного работника другому осуществляется только с разрешения соответствующего руководителя.

7.4. Исполненные документы с грифами "КТ", "К", "ДСП" или "ПД" группируются в дела в соответствии с номенклатурой дел, установленной Инструкцией по делопроизводству в Обществе. При этом на обложке дела, в которое помещены такие документы, также проставляется соответствующий гриф "КТ", "К", "ДСП" или "ПД".

7.5. Уничтожение дел, документов с грифом "КТ", "К", "ДСП" или "ПД", утративших свое практическое значение и не имеющих исторической ценности, производится по акту, который хранится у работника, ответственного за их уничтожение, назначаемого соответствующим Приказом.

7.6. Проверка наличия документов, дел и изданий с грифом "КТ", "К", "ДСП" или "ПД", а также соответствующих актов на их уничтожение может быть проведена комиссией, в составе заведующего секретариатом и представителей административного департамента, службы персонала и юридической службы. Результаты проверки оформляются актом.

7.7. В случаях утраты документов, дел и изданий, содержащих сведения конфиденциального характера, либо разглашения этих сведений, по распоряжению (указанию) Генерального директора Общества назначается комиссия для расследования обстоятельств утраты или разглашения. Результаты расследования представляются Генеральному директору Общества и по ним принимается решение о привлечении к ответственности виновных лиц либо об отказе в привлечении к ответственности.

На утраченные документы, дела и издания с грифом "КТ", "К", "ДСП" или "ПД" составляется соответствующий акт, который хранится в архиве Общества.

7.8. При снятии грифа "КТ", "К", "ДСП" или "ПД" с документов, об этом информируются все адресаты, которым эти документы были направлены.

## **8. ЗАЩИТА СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА ПРИ ОБРАБОТКЕ ИНФОРМАЦИИ НА СРЕДСТВАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ**

8.1. Сохранность сведений конфиденциального характера при их обработке на средствах вычислительной техники (СВТ) и передаче по компьютерным сетям Общества обеспечивается осуществлением комплекса организационных, технических и программных мер защиты информации.

8.2. Обязательными условиями обработки сведений конфиденциального характера на СВТ являются:

- персональный допуск пользователей к работе на СВТ в соответствии с установленным порядком;

- разграничение полномочий и доступа пользователей к информационным ресурсам автоматизированных и информационных систем корпоративной компьютерной сети (обеспечивается системными средствами разграничения, использованием индивидуальных идентификаторов и паролей, электронных ключей и т.п.);

- ведение учета всех электронных носителей конфиденциальной информации;

- обособленное хранение (в отдельных областях сетевых дисков, директориях, папках, файлах и т.п.) сведений конфиденциального характера с максимально возможным разграничением по доступу;

- создание резервных копий информационных массивов;

- стирание по минованию практической надобности информации и проектов документов, содержащих сведения конфиденциального характера, оставшихся на внешних запоминающих устройствах СВТ, а также очистка оперативной памяти путем выключения и перезагрузки компьютера после обработки сведений конфиденциального характера Общества;

- уничтожение информации с машинных носителей (уничтожение машинных носителей информации), на которые осуществлялась запись сведений конфиденциального характера, в случае выхода их из строя или непригодности (нецелесообразности) для дальнейшего использования, а также при плановой или внеплановой замене СВТ, в том числе при обновлении парка компьютеров;

- отключение на компьютерах работников Общества внешних устройств записи информации (накопителей на гибких магнитных дисках (дискетах), приводов CD-RW, USB-

портов и т.п. устройств записи информации). В случае производственной необходимости подключение таких устройств на компьютерах работников, которые по роду исполнения своих должностных обязанностей должны производить запись (копирование) информации, осуществляется Департаментом информационных технологий на основании заявки руководителя структурного подразделения;

- организация обособленной установки серверного и коммуникационного оборудования в отдельных, специально выделенных помещениях (серверных), которые должны находиться под постоянной охранной сигнализацией и вход в которые должен быть максимально ограничен;
- регистрация печатных копий и электронных носителей документов, содержащих сведения конфиденциального характера;
- исключение несанкционированного доступа к информационным массивам, содержащим сведения конфиденциального характера;
- недопущение передачи сведений конфиденциального характера по незащищенным каналам связи.

## **9. ЗАЩИТА РЕЧЕВЫХ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ**

9.1. Сохранность речевых сведений конфиденциального характера от утечки по техническим каналам достигается выполнением следующих основных мероприятий и требований:

- документальное определение перечня помещений (защищаемые помещения), специально предназначенных для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.);
- обеспечение режимных мер доступа в защищаемые помещения, к техническим средствам передачи и обработки информации, к кабельным коммуникациям;
- ведение переговоров, совещаний по вопросам, содержащим сведения конфиденциального характера, в защищаемых помещениях (по защищенным каналам связи);
- проведение периодического контроля состояния защиты информации в защищаемых помещениях;
- проведение, по решению руководства Общества, специальных проверок и специальных исследований помещений, технических средств, применяемых для обработки сведений конфиденциального характера, либо устанавливаемых в защищаемых помещениях. Средства аудио- и видеозаписи, аппаратура звукоусиления, используемые для обработки сведений конфиденциального характера, должны проходить специальную проверку и специальные исследования в обязательном порядке;
- запрещение использования во время проведения конфиденциальных мероприятий в защищаемых помещениях радиотелефонов (радиостанций), телефонов сотовой связи, мобильных компьютеров (ноутбуки и КПК);
- применение сертифицированных средств защиты сведений конфиденциального характера;

9.2. Ответственность за соблюдением требований по защите сведений конфиденциального характера возлагается на руководителей структурных подразделений, эксплуатирующих защищаемые помещения.

## **10. ТРЕБОВАНИЯ ПО ОБОРУДОВАНИЮ ПОМЕЩЕНИЙ И РАБОЧИХ МЕСТ**

10.1. Входные двери (окна) помещений, в которых производится обработка и хранение сведений конфиденциального характера, должны иметь замки (запоры), гарантирующие надежное их закрытие.

10.2. Порядок использования ключей (механических, электронных) должен исключать несанкционированный доступ в эти помещения посторонних лиц.

10.3. Для хранения сведений конфиденциального характера работники обеспечиваются сейфами (запирающимися шкафами), а также необходимым количеством папок и иной оргтехникой.

10.4. Обязательному закрытию и опечатыванию подлежат сейфы (запирающиеся шкафы) со сведениями конфиденциального характера и машинными носителями, размещающиеся в общих коридорах.

12.5. Наиболее важные помещения, в которых проводятся переговоры, совещания по вопросам, содержащим сведения конфиденциального характера, могут быть аттестованы на соответствие требованиям по безопасности информации.

10.6. Установка и замена оборудования, мебели, ремонт защищаемых помещений должны производиться по согласованию с Генеральным директором Общества.

## **11. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ПЕРЕДАЧИ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА СТОРОННИМ ОРГАНИЗАЦИЯМ**

11.1. Предоставление информации о деятельности Общества, а также, передача документов, содержащих сведения конфиденциального характера, органам государственной власти, иным государственным органам, органам местного самоуправления осуществляется в порядке, установленном законодательством Российской Федерации на основании мотивированного запроса, подписанного уполномоченным должностным лицом, с обязательным указанием данных о передаче на соответствующих документах грифа "КТ", "К", "ДСП" или "ПД".

11.2. Передача сведений конфиденциального характера контрагентам (юридическим или физическим лицам) Общества осуществляется на основании договора в объеме и на условиях, которые предусмотрены договором.

11.2.1. Соглашение о неразглашении сведений конфиденциального характера, определяющее условия конфиденциальности, срок их действия и порядок передачи сведений конфиденциального характера, заключается как неотъемлемое приложение к договору на выполнение работ (оказание услуг, поставки и т.п.). Допускается условия обеспечения конфиденциальности оформлять отдельным разделом договора.

11.2.2. Если при подготовке к заключению договора необходимо ознакомление контрагента со сведениями конфиденциального характера Общества, соглашение о неразглашении сведений конфиденциального характера заключается до передачи этих сведений и заключения основного договора, с последующим уточнением при необходимости условий конфиденциальности в соглашении о неразглашении сведений конфиденциального характера, заключаемом одновременно с основным договором. В этом случае соглашение о неразглашении сведений конфиденциального характера заключается и оформляется отдельным документом в соответствии с порядком, установленным в Обществе для заключения договоров.

11.2.3. Если при заключении Обществом договора предполагается, что в ходе выполнения работ будут разрабатываться конфиденциальные документы для их последующей передачи в Общество или другим юридическим или физическим лицам, то в соглашении о неразглашении сведений конфиденциального характера может предусматриваться передача контрагенту Перечня сведений конфиденциального характера в объеме, минимально необходимом для надлежащего исполнения этого договора.

11.2.4. Право подписи от имени Общества Соглашения о неразглашении сведений конфиденциального характера предоставляется Генеральному директору - на основании Устава, а также другим лицам - на основании доверенности, оформленной установленным порядком.

11.3. Предоставление сведений конфиденциального характера сторонним организациям, не являющимся контрагентами Общества, осуществляется на основании мотивированного запроса по письменному разрешению Генеральному директору Общества.

Предварительно руководитель структурного подразделения, которому поручено исполнение запроса, совместно с Департаментом информационных технологий в срок, не превышающий трех рабочих дней, проводит оценку обоснованности запроса, соответствия тематики и объема информации целям и задачам, которые должны решаться в результате ее получения.

11.4. Передача сторонним организациям и физическим лицам сведений конфиденциального характера контрагентов Общества, должна осуществляться с их

письменного согласия, на основании соответствующих запросов или заключенных договоров (соглашений, контрактов).

11.5. Передача сведений конфиденциального характера должна осуществляться, как правило, на бумажных носителях, если их передача на иных носителях не предусмотрена действующим законодательством Российской Федерации либо условиями заключенных договоров. В случае, когда подлежащие передаче документы содержат сведения конфиденциального характера, обязательно проставление на них соответствующего ограничительного грифа. На документах, содержащих сведения конфиденциального характера, дополнительно указывается наименование обладателя информации и его местоположение.

11.5.1. В случае обоснованной необходимости передача сведений конфиденциального характера на машинном носителе осуществляется с сопроводительным письмом, в соответствии с порядком, определенным в Обществе. В сопроводительном письме указываются перечень и ограничительный гриф отдельных файлов (информационных массивов), записанных на данном носителе. Гриф, проставляемый на самом машинном носителе, должен быть не ниже высшего ограничительного грифа информации, на нем записанной.

11.5.2. Передача сведений конфиденциального характера сторонним организациям на машинных носителях, в том числе запись информации на машинные носители принимающей стороны, без разрешения Генерального директора Общества или уполномоченных им лиц запрещается.

## **12. ПОРЯДОК ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ ОБЩЕСТВА РАБОТНИКОВ СТОРОННИХ ОРГАНИЗАЦИЙ**

12.1. Доступ командированных в Общество работников сторонних организаций к сведениям конфиденциального характера и документам осуществляется решением Генерального директора Общества в объеме, необходимом исключительно для выполнения задач командировки.

12.2. Доступ к ресурсам электронных информационных систем осуществляется на основании заявки, оформляемой порядком и по форме, установленным для работников Общества. Заявка подписывается Генеральным директором Общества, руководителем соответствующего структурного подразделения, в которое прибыл командированный работник, и согласовывается с Управлением по информационным технологиям.

12.3. Непосредственный доступ к ресурсам электронных информационных систем осуществляет Департамент информационных технологий.

12.4. В общем порядке доступ представителей сторонних организаций, а также физических лиц, оказывающих услуги (выполняющих работы) Обществу, к электронным источникам информации запрещен.

12.4.1. К совершению отдельных операций с использованием электронных информационных систем Общества представители сторонних организаций допускаются на основании заключенных договоров или с письменного разрешения Генерального директора Общества или лица, его замещающего.

12.4.2. На представителей сторонних организаций, допускаемых к совершению отдельных операций с использованием электронных информационных систем Общества, оформляется заявка в соответствии с порядком и по форме, которые установлены для работников Общества.

12.4.3. На каждого представителя контрагента Управлением по информационным технологиям оформляется отдельная учетная запись в порядке, установленном соответствующими регламентами.

Примечание: данный порядок доступа к электронным информационным системам Общества распространяется и на представителей органов государственной власти, иных государственных органов, выполняющих свои функции в соответствии с действующим законодательством Российской Федерации.

12.5. Контроль соблюдения представителями сторонних организаций установленного в Обществе режима охраны сведений конфиденциального характера при использовании электронных информационных систем возлагается на руководителей структурных подразделений, к которым прибыли представители.

### **13. ОПУБЛИКОВАНИЕ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА В СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ**

13.1. Запрещается публикация сведений конфиденциального характера в средствах массовой информации, включая Интернет и другие публичные компьютерные сети, а также использование их в публичных выступлениях до снятия в установленном порядке существующих ограничений.

13.2. Возможность открытого оглашения (публикации) сведений конфиденциального характера, владельцем которых является Общество, определяется решением Генерального директора Общества.

Открытое оглашение (публикация) сведений конфиденциального характера, в отношении которых Общество не является владельцем (собственником), может осуществляться при наличии письменного согласия владельца (собственника) этих сведений конфиденциального характера на их открытое оглашение (публикацию), а также в иных случаях, предусмотренных действующим законодательством Российской Федерации.

13.3. В случае принятия такого решения и открытого оглашения (публикации) сведений:

- сведения утрачивают статус конфиденциальности, в отношении этих сведений утрачивает действие режим охраны сведений конфиденциального характера, установленный в Обществе Положением и другими разработанными на его основе нормативными документами;
- на документах, содержащих эти сведения, ограничительный гриф снимается;
- в отношении этих сведений утрачивается действие обязательства и условия конфиденциальности в действующих договорах (соглашениях, контрактах), заключенных ранее.

13.4. Появление в средствах массовой информации сведений конфиденциального характера, в порядке, отличном от описанного в п. 14.2 Положения, а также использование ноу-хау Общества другими юридическими и физическими лицами не означает выполнения по отношению к этим сведениям мероприятий, изложенных в п. 14.3 Положения.

13.5. При публикации в средствах массовой информации, включая Интернет и другие публичные компьютерные сети, статей, касающихся деятельности и/или сведений конфиденциального характера Общества, работники - авторы статей обязаны соотносить используемый в публикациях материал с действующим в Обществе Перечнем сведений конфиденциального характера.

13.5.1. Перед публикацией статьи должны обязательно согласовываться (рецензироваться) с Генеральным директором Общества с указанием в рецензиях фразы: "Использованные в статье материалы сведений конфиденциального характера не содержат".

13.6. Работники, обнаружившие факт публикации в средствах массовой информации, включая Интернет, а также использования в публичных выступлениях сведений конфиденциального характера, обязаны сообщить об этом своему непосредственному руководителю.

### **14. АРХИВНОЕ ХРАНЕНИЕ**

14.1. Документы или иные носители сведений конфиденциального характера в случаях утраты их оперативной важности для деятельности Общества и в иных случаях, предусмотренных законодательством РФ, передаются на хранение в архив.

14.2. Архивное хранение документов, содержащих сведения конфиденциального характера, осуществляется на основании настоящего Положения, Инструкции по организации и ведению делопроизводства, локальных нормативных актов Общества и законодательства РФ.

14.3. В случае, если с переданных документов или иных носителей сведений конфиденциального характера не был снят гриф конфиденциальности, то доступ к сведениям, содержащимся в таких документах, осуществляется в порядке, предусмотренном в настоящем Положении, Инструкции по организации и ведению делопроизводства и иных локальных нормативных актах Общества.

14.4. Лицо, ответственное за архивное хранение сведений конфиденциального характера, устанавливается в Инструкции по организации и ведению делопроизводства.

## 15. ПОРЯДОК ДОПУСКА РАБОТНИКОВ К СВЕДЕНИЯМ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, И ПРЕКРАЩЕНИЯ ДОПУСКА

15.1. Основанием для допуска работников к сведениям конфиденциального характера является приказ о принятии на работу либо заключение договора гражданско-правового характера.

15.2. До издания приказа с кандидатом на работу оформляется два экземпляра обязательства о неразглашении сведений конфиденциального характера. Один экземпляр обязательства передается работнику, второй приобщается к материалам личного дела.

15.3. После издания приказа и до предоставления фактического доступа работника к сведениям конфиденциального характера, руководитель структурного подразделения, в которое поступает работник:

- доводит до работника под расписку требования Положения и Перечень сведений конфиденциального характера ООО «ВЫСОТКА», а также других документов, регламентирующих порядок работы со сведениями конфиденциального характера;

- предупреждает об ответственности за нарушение установленного в Обществе порядка обращения со сведениями конфиденциального характера;

- передает работнику копию Памятки по обеспечению сохранности сведений конфиденциального характера.

15.4. Организация доступа работника к информационным ресурсам электронных вычислительных систем Общества регулируется Регламентом предоставления доступа к информационным ресурсам и осуществляется Департаментом информационных технологий..

15.5. Фактический доступ работника к документам, машинным носителям и информационным ресурсам электронных вычислительных систем Общества, содержащим сведения конфиденциального характера, в объеме, необходимом для исполнения им должностных обязанностей, организует его непосредственный руководитель.

15.6. Обязанность работника соблюдать требования настоящего Положения, а также ответственность за разглашение сведений конфиденциального характера отражается в заключаемом с ним трудовом договоре.

15.7. Основанием для прекращения доступа к сведениям конфиденциального характера является:

- приказ об увольнении работника;

- заявление работника об увольнении либо объявление работнику в соответствии с трудовым законодательством о предстоящем увольнении (в этом случае необходимость и объем работы со сведениями конфиденциального характера на период до издания приказа определяет заместитель Генерального директора Общества по направлению деятельности);

- нарушение работником взятых на себя обязательств, связанных с неразглашением сведений конфиденциального характера;

- решение Генерального директора Общества об отстранении работника от работы со сведениями конфиденциального характера. Решение оформляется приказом и доводится до сведения работника под роспись.

15.8. При наличии одного из перечисленных оснований непосредственный руководитель работника, доступ которого к сведениям конфиденциального характера прекращен, обязан незамедлительно сообщить об этом в Департамент информационных технологий.

15.9. При увольнении работника за допущенное нарушение трудовой дисциплины, своих обязательств по трудовому договору с Обществом или в иных случаях, предусмотренных законом, без согласия работника служба по работе с персоналом незамедлительно информирует о данном факте непосредственного руководителя увольняемого работника и **Департамент информационных технологий** для принятия мер по ограничению доступа работника к информационным ресурсам, содержащим сведения конфиденциального характера.

## **16. ОБЯЗАННОСТИ РАБОТНИКОВ, ДОПУЩЕННЫХ К СВЕДЕНИЯМ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА**

16.1. Работники Общества, допущенные к сведениям конфиденциального характера, обязаны:

- знать и выполнять требования Положения и других нормативных документов Общества, регламентирующих вопросы обеспечения режима охраны сведений конфиденциального характера и порядка обращения со сведениями конфиденциального характера;
- не разглашать сведениям конфиденциального характера, полученные в результате выполнения своих должностных обязанностей;
- соблюдать установленные в Обществе правила работы с документами, порядок их учета, хранения и уничтожения;
- знакомиться только с теми документами и информацией, к которым получили допуск в силу своих должностных обязанностей;
- во время работы с документами принимать меры к исключению возможности ознакомления с ними других лиц, не имеющих к ним прямого отношения;
- пресекать действия других лиц, которые могут привести к разглашению сведений конфиденциального характера;
- при составлении документов ограничиваться минимальными, действительно необходимыми сведениями конфиденциального характера;
- определять количество экземпляров документа в строгом соответствии со служебной необходимостью;
- документы, содержащие сведения конфиденциального характера и находящиеся на исполнении (не подшитые в дела), хранить в отдельной папке;
- в нерабочее время, а также при кратковременном отсутствии на рабочем месте документы, содержащие сведения конфиденциального характера, хранить в закрытом на замок шкафу (сейфе);
- документы с грифами "КТ" и "К" после их исполнения группировать (подшивать) в дела, предусмотренные номенклатурой дел структурного подразделения, в соответствии с порядком, установленным в Обществе;
- немедленно информировать руководителя структурного подразделения и директора Департамента информационных технологий о фактах утраты (недостачи) документов (отдельных листов), содержащих сведения конфиденциального характера, ключей от сейфов (шкафов), фактах обнаружения неучтенных документов, а также о фактах необоснованного интереса к сведениям конфиденциального характера со стороны лиц, не имеющих прямого отношения к работе с ними;
- при увольнении, переводе по работе, убытии в отпуск, длительную командировку (более 1 месяца) сдать документы, содержащие сведения конфиденциального характера.

16.2. При обработке сведений конфиденциального характера с использованием средств вычислительной и оргтехники работники обязаны:

- соблюдать правила разграничения доступа к охраняемым данным, неукоснительно выполнять требования нормативных документов по организации доступа к информационным ресурсам, организации парольной и антивирусной защиты;
- не разглашать свои индивидуальные пароли на доступ к компьютерным, сетевым и иным информационным ресурсам, выполнять требования соответствующих администраторов вычислительной сети и администраторов автоматизированных (информационных) систем по смене паролей, не применять "простых" паролей, не оставлять в легкодоступных местах листы и конверты с паролями;
- принимать меры к исключению ознакомления посторонних лиц с информацией, выводимой на экран дисплея;
- при подготовке электронных документов, содержащих сведения конфиденциального характера, в верхнем правом углу (колоннитуле) первого экранного листа проставлять пометку с соответствующим ограничительным грифом ("Коммерческая тайна" или "Конфиденциально"). При этом на документах с ограничительным грифом "Коммерческая тайна" ниже его дополнительно указывать наименование обладателя этой информации, за



исключением случаев, когда электронный документ подлежит выводу на бланки, на которых уже указан обладатель сведений конфиденциального характера;

- не использовать (не загружать, не запускать и т.п.) для обработки сведений конфиденциального характера посторонние программные средства, не допущенные для применения в Обществе. При требовании операционной системы обновления установленного программного обеспечения обязательно его произвести;

- при необходимости покинуть свое рабочее место провести стандартные процедуры выхода из системы и отключения компьютера (в рабочее время допускается инициализация экранной заставки, защищенной индивидуальным паролем, или блокировка доступа к компьютеру с использованием аппаратно-программных средств и электронных ключей, принятых для эксплуатации в Обществе);

- не допускать случаев передачи сведений конфиденциального характера по незащищенным каналам передачи данных, через сеть Интернет и иные публичные сети (включая факс), по электронной почте в открытом виде;

- не допускать применения средств криптографической защиты и защиты от несанкционированного доступа, не принятых в эксплуатацию в Обществе или не предусмотренных эксплуатационной (технической) документацией на информационные и автоматизированные системы;

- в нерабочее время, а также при кратковременном отсутствии на рабочем месте хранить съемные машинные носители, содержащие сведения конфиденциального характера, в закрытом на замок сейфе (шкафу);

- немедленно информировать руководителя структурного подразделения о фактах или возможности несанкционированного доступа к сведениям конфиденциального характера в локальной вычислительной сети (ЛВС) Общества.

16.3. Работникам, допущенным к сведениям конфиденциального характера, запрещается:

- снимать и изготавливать копии документов (в том числе с электронных документов), делать из них выписки без разрешения руководителя структурного подразделения;

- выносить за пределы здания Общества документы и машинные носители со сведениями конфиденциального характера без разрешения руководителя своего подразделения. В случае служебной необходимости выноса (вывоза) документов и носителей, содержащих сведения конфиденциального характера, на срок командировки разрешение должно получаться у заместителя директора по безопасности или Генерального директора Общества. При этом в служебной записке указывается перечень сведений конфиденциального характера;

- работать со сведениями конфиденциального характера вне служебных помещений;

- обсуждать сведения конфиденциального характера в присутствии посторонних лиц;

- сообщать устно или письменно кому бы то ни было сведения конфиденциального характера, если это не обусловлено выполнением служебных обязанностей.

16.3.1. Кроме того, работникам Общества запрещается:

- подключать к компьютерам различного рода внешние устройства, устанавливать на компьютеры и (или) использовать программные продукты (программы), копировать на (с) внешние машинные носители программное обеспечение без разрешения руководителя подразделения, за исключением программного обеспечения, устанавливаемого в соответствии с нормативными документами Общества;

- самостоятельно, без разрешения руководителя подразделения, подключать (или допускать подключение) к ЛВС Общества компьютеры (в том числе мобильные) представителей контрагентов и других организаций или физических лиц, прибывающих в Общество;

- вносить без разрешения руководителя подразделения в пределы охраняемой территории Общества и использовать без согласования для обработки сведений конфиденциального характера личные компьютеры (ноутбуки);

- использовать для сохранения сведений конфиденциального характера, личные (не принадлежащие Обществу) компьютеры (в том числе мобильные - ноутбуки, карманные персональные компьютеры (КПК), электронные записные книжки, смартфоны, мобильные телефоны и другие мобильные цифровые (вычислительные) устройства);

- использовать средства корпоративной электронной почты для отправки неслужебной корреспонденции, сообщать персональные электронные почтовые адреса для получения неслужебной корреспонденции (в том числе электронных рассылок) через сеть Интернет.

## **17. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, УТРАТУ СОДЕРЖАЩИХ ИХ ДОКУМЕНТОВ**

17.1 Разглашение сведений конфиденциального характера или утрата документов, содержащих таковые, относится к числу грубых нарушений трудовых обязанностей.

17.2. За разглашение сведений конфиденциального характера, утрату документов, содержащих такие сведения, а также за иные аналогичные виновные лица несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

17.3. По фактам разглашения (утраты) сведений конфиденциального характера и/или по фактам грубого нарушения установленных в Обществе правил обращения со сведениями конфиденциального характера, проводится служебное расследование.

Для проведения служебного расследования приказом Генерального директора Общества назначается комиссия в составе не менее трех человек.

Руководитель структурного подразделения, проверяемого по фактам разглашения (утраты) сведений конфиденциального характера принимает активное участие в обеспечении работы комиссии.

17.4. Комиссия, проводящая служебное расследование:

- выясняет обстоятельства, причины разглашения сведений или утраты документов, грубых нарушений, а также способствовавшие этому условия;

- устанавливает лиц, виновных в разглашении сведений или утрате документов, грубых нарушениях;

- принимает меры к розыску утраченного документа или предотвращению негативных последствий разглашения сведений, грубых нарушений.

17.5. Члены комиссии, проводящие служебное расследование, имеют право:

- производить осмотр помещений Общества (сейфов, столов, шкафов, и т.д.);

- проверять конфиденциальную документацию, журналы учета конфиденциальных документов;

- опрашивать работников Общества, виновных в утрате (разглашении) и/или грубых нарушениях, а также других работников Общества, могущих оказать содействие в установлении обстоятельств происшедшего и получать от них письменные объяснения;

- привлекать работников других структурных подразделений, не заинтересованных в исходе дела, для проведения отдельных действий служебного расследования по согласованию с их руководителями.

17.6. Служебное расследование проводится в минимально короткий срок, но не более 10 рабочих дней со дня назначения комиссии. В случаях, когда в течение данного срока утраченные документы не обнаружены, поиск их может быть прекращен.

17.7. По результатам расследования составляется заключение, в котором отражаются следующие вопросы:

- основания для проведения расследования;

- кто и в какие сроки проводил расследование;

- перечень и результаты осуществленных мероприятий;

- виновные лица;

- выявленные причины и условия, способствовавшие разглашению (утрате);

- мнение о наличии в действиях виновного лица признаков административного правонарушения либо уголовно наказуемого деяния;

- возможные негативные последствия происшедшего для интересов Общества и предложения по их устранению.

17.8. Заключение по результатам служебного расследования докладывается Генеральному директору Общества для принятия решения о привлечении виновного к дисциплинарной

ответственности либо о передаче материалов в правоохранительные или судебные органы, а также о мерах по устранению причин и возможных негативных последствий происшедшего либо об отклонении материалов расследования.

### **18. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

18.1. Настоящее Положение вступает в силу с момента его утверждения Генеральным директором и действует до введения нового Положения или иных документов, регулирующих отдельные вопросы данного Положения.

18.2. В случае принятия иных документов, регулирующих отдельные вопросы данного Положения, настоящее Положение утрачивает силу лишь в части этих вопросов, что закрепляется в соответствующем приказе Генерального директора.

18.3. Ознакомление работников с условиями настоящего Положения производится под роспись в листе ознакомления. Подписание работником листа ознакомления с Положением означает его согласие и обязательство исполнения требований Положения.

18.4. Одновременно с подписанием листа ознакомления работник подписывает 2 экземпляра Обязательства о неразглашении сведений конфиденциального характера. Один экземпляр Обязательства хранится в Службе персонала Общества, второй под роспись передается на руки работнику.

18.5. Настоящее Положение включает в себя:

#### **ПРИЛОЖЕНИЯ:**

Приложение 1 - ПЕРЕЧЕНЬ сведений конфиденциального характера ООО «ВЫСОТКА»

Приложение 2 – ПАМЯТКА Работнику о сохранении сведений конфиденциального характера

Приложение 3 – ОБЯЗАТЕЛЬСТВО о неразглашении сведений конфиденциального характера

**ПЕРЕЧЕНЬ**  
**Сведений конфиденциального характера**  
**ООО «ВЫСОТКА»**

1. Перечень сведений, составляющих коммерческую тайну
  - 1.1. Сведения в области экономики и финансов
    - 1.1.1. Сведения, содержащиеся в первичных документах бухгалтерского и налогового учета, промежуточных финансовых отчетах, экономических расчетах, результатах финансово-экономических экспертиз;
    - 1.1.2. Сведения об открытых в кредитных учреждениях расчетных и иных счетах, в том числе в иностранной валюте, о движении средств по этим счетам, и об остатке средств на этих счетах, сведения об имеющихся вкладах в банках, в том числе в иностранной валюте (банковская тайна);
    - 1.1.3. Сведения о планах инвестиций, о наиболее выгодных финансовых вложениях в ценные бумаги, акции, недвижимое имущество и др.;
    - 1.1.4. Сведения о подготовке к торгам или аукциону и их результатах.
  - 1.2. Сведения в области производства и реализации продукции и услуг
    - 1.2.1. Сведения о разрабатываемых пакетах услуг, новых тарифах, новых услуг ресторанов, новых блюдах и пр.
    - 1.2.2. Сведения о целях, задачах, тактике и стратегии ведения переговоров с деловыми партнерами.
    - 1.2.3. Сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, клиентах, потребителях, покупателях, компаньонах, спонсорах, посредниках и других партнерах, а также конкурентах, которые не содержатся в открытых источниках (справочниках, каталогах и др.).
    - 1.2.4. Сведения об условиях договоров, их предмете, содержании, ценах и других существенных условиях.
    - 1.2.5. Сведения о методах расчета, структуре, уровне цен на продукцию и услуги, размерах скидок.
    - 1.2.6. Сведения о планах и применяемых методах осуществления закупок и продаж.
  - 1.3. Сведения в области маркетинговых исследований
    - 1.3.1. Сведения о способах и методах проведения маркетинговых исследований, применяемых методиках анализа конкурентной среды.
    - 1.3.2. Сведения о результатах маркетинговых исследований, содержащие оценки состояния и перспективы развития рыночной конъюнктуры.
    - 1.3.3. Сведения об эффективности коммерческой деятельности.
    - 1.3.4. Сведения о стратегии развития и маркетинговой политике.
  - 1.4. Сведения о состоянии и способах сведений конфиденциального характера
    - 1.4.1. Сведения о порядке организации охраны, пропускном режиме, системе допуска к сведениям конфиденциального характера.
    - 1.4.2. Сведения о системе сигнализации и технических способах контроля доступа к сведениям конфиденциального характера.

2. Перечень сведений, составляющих служебную тайну
  - 2.1. Сведения о применяемых методах управления и наиболее ценных управленческих решениях.
  - 2.2. Сведения о подготовке, принятии и исполнении решений.
  - 2.3. Сведения о целях, рассматриваемых вопросах, результатах, фактах проведения совещаний и заседаний.
  - 2.4. Сведения, содержащиеся в распорядительных документах, протоколах, соглашениях, а также в их проектах и вариантах.
  - 2.5. Сведения с грифом ограничения доступа, поступившие в Общество.
  - 2.6. Сведения о порядке и состоянии защиты служебной тайны, включая сведения о системе допуска к служебной тайне, системе сигнализации и технических способах контроля доступа к служебной тайне.

3. Перечень сведений, составляющих персональные данные
  - 3.1. Все сведения, упомянутые в Положении об обработке и защите персональных данных в ООО «ВЫСОТКА», утвержденном соответствующим Приказом по Обществу.

## **ПАМЯТКА Работнику о сохранении сведений конфиденциального характера**

В условиях рыночной экономики и конкурентных отношений сведения конфиденциального характера выступают как элемент маркетинговой политики и как способ увеличения прибыли ООО «ВЫСОТКА» (далее по тексту Общество).

Утечка сведений конфиденциального характера может привести к снижению доходов Общества.

Работник Общества обязан строго хранить в тайне сведения конфиденциального характера, ставшие ему известными в связи с выполнением трудовых обязанностей.

Разглашение сведений конфиденциального характера, передача их третьим лицам без согласия Общества, а также использование указанных сведений для занятия любой деятельностью, которая, как конкурентное действие, может нанести ущерб Обществу, влечет уголовную, административную, гражданскую и иную ответственность в соответствии с действующим законодательством РФ.

Порядок обращения со сведениями конфиденциального характера, а также перечни указанных сведений установлены Положением о сведениях конфиденциального характера в ООО «ВЫСОТКА».

Работник обязан работать только с теми сведениями и документами конфиденциального характера, к которым он допущен в силу служебных обязанностей, а также должен знать, кому из других работников Общества разрешено работать со сведениями конфиденциального характера, к которым он сам допущен.

При участии в работе сторонних организаций работник может знакомить их представителей со сведениями конфиденциального характера только с письменного разрешения руководителя соответствующего структурного подразделения.

В письменном разрешении должны быть определены конкретные вопросы, подлежащие рассмотрению, а также указано кому и в каком объеме могут быть доведены сведения, подлежащие защите.

Об утрате или недостаче документов, содержащих сведения конфиденциального характера, пропусков, ключей от служебных и архивных помещений, сейфов, металлических шкафов, печатей, а также о причинах и условиях возможной утечки таких сведений работник обязан немедленно сообщить своему непосредственному руководителю и/или руководителю Административного департамента.

Работник обязан по первому требованию непосредственного руководителя или специально созданной комиссии из числа работников соответствующих структурных подразделений предъявлять для проверки все числящиеся за ним материалы, содержащие сведения конфиденциального характера (документы, черновики, магнитные носители и т.п.), представлять устные или письменные объяснения о нарушениях установленных правил обращения с конфиденциальными материалами, а также о фактах разглашения сведений конфиденциального характера, утраты документов, содержащих такие сведения.

В случае попытки посторонних лиц или организаций получить сведения конфиденциального характера работник обязан сообщить об этом своему непосредственному руководителю и/или руководителю Административного департамента.

При прекращении допуска работника к сведениям конфиденциального характера в связи с его переводом на другую должность или при увольнении из Общества, работник обязан передать все находящиеся у него документы, содержащие такую информацию, своему непосредственному руководителю или другому работнику, определенному непосредственным руководителем.

С Памяткой о сохранении сведений конфиденциального характера ознакомлен.

Инструктаж о порядке работы со сведениями конфиденциального характера получил.

Об ответственности за разглашение сведений конфиденциального характера предупрежден.

\_\_\_\_\_ / \_\_\_\_\_ « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.  
подпись    Фамилия, И.О.

**ОБЯЗАТЕЛЬСТВО**  
**о неразглашении сведений конфиденциального характера**

Я, \_\_\_\_\_, в качестве  
работника ООО «ВЫСОТКА» в период трудовых отношений с ООО «ВЫСОТКА» (его  
правопреемником) и в течение 3 (Трех) лет после их окончания, в соответствии с трудовым  
договором, \_\_\_\_\_ заключенным \_\_\_\_\_ между \_\_\_\_\_ мной  
и ООО «ВЫСОТКА», а также  
соответствующими положениями по обеспечению сохранности сведений конфиденциального  
характера, действующих в ООО «ВЫСОТКА»,

**ОБЯЗУЮСЬ:**

- 1) не разглашать сведения конфиденциального характера, которые мне будут доверены или станут известны по работе;
- 2) не передавать третьим лицам и не раскрывать публично сведения конфиденциального характера, без согласия администрации ООО «ВЫСОТКА»;
- 3) выполнять относящиеся ко мне требования приказов, инструкций и положений по обеспечению сохранности сведений конфиденциального характера ООО «ВЫСОТКА»;
- 4) в случае попытки посторонних лиц получить от меня сведения конфиденциального характера немедленно сообщить своему непосредственному руководителю;
- 5) сохранять сведения конфиденциального характера тех контрагентов, у которых имеются деловые отношения с ООО «ВЫСОТКА»;
- 6) не использовать знание сведений конфиденциального характера ООО «ВЫСОТКА» для занятий любой деятельностью, которая в качестве конкурентного действия может нанести ущерб ООО «ВЫСОТКА»;
- 7) в случае моего увольнения, в последний рабочий день (если непосредственный руководитель не обяжет сделать это раньше), все носители сведений конфиденциального характера ООО «ВЫСОТКА» (рукописи, черновики, чертежи, диски, дискеты, цифровые носители, распечатки на принтерах, кино-, фотонегативы и позитивы, модели, материалы, изделия и т.п.), которые находились в моем распоряжении в связи с выполнением мною должностных обязанностей во время работы в ООО «ВЫСОТКА», передать своему непосредственному руководителю;
- 8) об утрате или недостатке носителей сведений конфиденциального характера, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению данных сведений ООО «ВЫСОТКА», а также о причинах и условиях возможной утечки сведений немедленно сообщать своему непосредственному руководителю.

Я предупрежден, что в случае невыполнения любого из пунктов 1, 2, 3, 4, 5, 6, 8 настоящего обязательства могу быть уволен в соответствии с подп. «В» пункта 6 статьи 81 ТК РФ.

До моего сведения также доведены с разъяснениями соответствующие положения по обеспечению сохранности сведений конфиденциального характера ООО «ВЫСОТКА».

Мне известно, что нарушение этих положений может повлечь уголовную, административную, гражданско-правовую или иную ответственность, предусмотренную действующим законодательством Российской Федерации, в виде лишения свободы, денежного штрафа, обязанности по возмещению ущерба ООО «ВЫСОТКА» (убытков, упущенной выгоды).

" \_\_\_\_ " \_\_\_\_\_ 20 \_\_\_\_ г.

\_\_\_\_\_ (подпись)

Второй экземпляр данного документа на руки получил " \_\_\_\_ " \_\_\_\_\_ г.

\_\_\_\_\_ (подпись)