Приложение № 1
к приказу № 130 от 11.07.2019

ПОЛОЖЕНИЕ

О КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

Публичного акционерного общества
«Центральное конструкторское бюро «Айсберг»
(ПАО «ЦКБ «Айсберг»)

Санкт-Петербург
2019

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

Коммерческая тайна (КТ) – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Информация, составляющая коммерческую тайну – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании, и в отношении которых обладателем таких сведений введен режим конфиденциальности.

Обладатель информации, составляющей коммерческую тайну – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

Режим конфиденциальности – правовые, организационные, технические и иные меры, принимаемые обладателем информации, к охране информации ограниченного доступа, включая коммерческую тайну, персональные данные и иную, охраняемую в соответствии с законодательством Российской Федерации, а также нормативными актами и документами Общества информацию.

Доступ к информации, составляющей коммерческую тайну – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача информации, составляющей коммерческую тайну – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Контрагент – юридическая сторона, с которой организация заключает договор или находится в договорных отношениях, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию.

Информация ограниченного доступа – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления, составляющие коммерческую тайну, или иные сведения, охраняемые в соответствии с законодательством Российской Федерации, а также нормативными актами и документами Общества.

Передача информации ограниченного доступа – доведение ее обладателем в документированном виде до уполномоченных штатных работников получающей стороны и принятие ими установленных законом или договором мер по охране ее конфиденциальности.

Конфиденциальный документ – зафиксированная на материальном носителе информация ограниченного доступа с реквизитами, позволяющими ее идентифицировать.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному, или определяемому физическому лицу (субъекту персональных данных).

Предоставление информации, составляющей коммерческую тайну – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение информации, составляющей коммерческую тайну – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и т.п.).

Информационные системы персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Гриф конфиденциальности – реквизиты, свидетельствующие о степени конфиденциальности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

Применяемые в Обществе грифы конфиденциальности:

- **Коммерческая тайна** – гриф конфиденциальности для документов, содержащих информацию, составляющую коммерческую тайну Общества.
- **Для служебного пользования (ДСП)** – гриф конфиденциальности, для документов, содержащих служебную информацию, не относящуюся к сведениям, составляющим коммерческую тайну и персональные данные.

Носители сведений, составляющих коммерческую тайну – материальные объекты, в том числе физические поля, в которых сведения, составляющие коммерческую тайну, находят свое отображение в виде символов, образов, сигналов, моделей, технических решений и процессов.

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированных систем.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее «Положение о защите конфиденциальности информации Публичного акционерного общества «Центральное конструкторское бюро «Айсберг» (далее – Положение) определяет единый режим конфиденциальности и является основным руководящим документом, обязательным для исполнения всеми структурными подразделениями Публичного акционерного общества (далее – Общество) по формированию режима конфиденциальности в процессе ведения уставной деятельности, и содержит необходимый набор требований, мероприятий, действий и методик, которые необходимо осуществить и применять структурным подразделениям Общества в целях обеспечения сохранности конфиденциальной информации Общества.

1.2. Режим конфиденциальности определяется:

— Перечнем защищаемых информационных ресурсов информационных систем персональных данных Общества.

— Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных;

— Положением об обработке персональных данных;

— Перечнем сведений, составляющих коммерческую тайну;

— Настоящим положением;

— Установленным порядком отнесения информации к коммерческой тайне (Раздел 4 настоящего Положения).

1.3. В соответствии с настоящим Положением Общество принимает меры к обеспечению конфиденциальности информации ограниченного доступа.

1.4. В случае если, в связи с осуществлением своей деятельности, Обществу становятся известны сведения, составляющие в соответствии с законодательством РФ защищаемую законом тайну, Общество обязано предпринимать меры по их охране, в соответствии с федеральным законом Российской Федерации от 29.07.2004 №98-ФЗ «О коммерческой тайне», и иными нормативными правовыми актами о защищаемой законом тайне.

1.5. Действие настоящего Положения распространяется на все структурные подразделения Общества, в том числе обособленные – филиалы и представительства.

1.6. Требования к мерам, необходимым и достаточным для обеспечения выполнения обязанностей Общества, предусмотренных законодательством Российской Федерации в области персональных данных, при осуществлении обработки персональных данных, определены в «Положении об обработке персональных данных ПАО «ЦКБ «Айсберг».

1.7. Требования к мероприятиям по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, предусмотренных законодательством Российской Федерации в области персональных данных, определены в «Положении об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных «ПАО «ЦКБ «Айсберг».

1.8. Требования к мероприятиям по обеспечению безопасности служебной информации ограниченного доступа, имеющей гриф конфиденциальности, и не относящуюся к сведениям, составляющим коммерческую тайну, и персональным данным, определены в «Технологической инструкции администратору безопасности информации по выполнению работ в Автоматизированной системе обработки конфиденциальной информации ПАО «ЦКБ «Айсберг» и «Технологической инструкции пользователя безопасности информации по выполнению работ в Автоматизированной системе обработки конфиденциальной информации ПАО «ЦКБ «Айсберг».

1.9. Настоящее Положение включает требования по обеспечению комплекса (системы) мер, обеспечивающих функционирование режима конфиденциальности, включающего:

— принятие локальных нормативных актов, определяющих порядок работы с носителями, содержащими информацию ограниченного доступа, в т.ч. сведения, составляющие КТ, права и обязанности структурных подразделений и исполнителей Общества, имеющих отношение к работе с указанной информацией (сведениями);

— административные и организационные меры по обеспечению реализации регламентов и локальных нормативных актов;

— программно-технические меры, обеспечивающие защиту информации ограниченного доступа при обработке её в автоматизированных информационных системах Общества.

1.10. Построение режима конфиденциальности осуществляется на следующих принципах:

— соблюдение законодательства в области защиты информации ограниченного доступа и, в частности, защиты сведений, составляющих КТ;

— обязательное выполнение работниками Общества сформированных данным Положением требований по защите информации ограниченного доступа;

— выполнение условий достаточности и экономической обоснованности внедрения дополнительных мер по защите информации ограниченного доступа;

— сведения, составляющие КТ, для которых вводится режим конфиденциальности, должны сохранять свойства коммерческой значимости (актуальности), целостности, достоверности и возможность их использования в целях решения экономических интересов Общества.

1.11. Положение включает требования по обеспечению конфиденциальности информации, в соответствии с частью 1 ст.10 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне», которые состоят в следующем:

1.11.1. Разработка критериев отнесения информации к коммерчески значимой, подготовка и определение «Перечня сведений, составляющей коммерческую тайну».

1.11.2. Разработка локальных нормативных актов, минимально необходимых для создания режима конфиденциальности.

1.11.3. Введение порядка передачи информации ограниченного доступа, в т.ч. сведений, составляющих КТ, между Обществом и внешними контрагентами в процессе договорных отношений.

1.11.4. Введение ограничений доступа к информации, путем установления порядка обращения с этой информацией и контроля за соблюдением установленных требований.

1.11.5. Создание правовой основы, регулирующей отношения по использованию информации ограниченного доступа, в т.ч. сведений, составляющей КТ, с работниками на основе трудовых договоров.

1.11.6. Создание системы подготовки и повышения квалификации работников подразделений Общества, занимающихся обеспечением режима конфиденциальности.

2. ОРГАНИЗАЦИОННАЯ ОСНОВА И ФУНКЦИИ ДОЛЖНОСТНЫХ ЛИЦ ОБЩЕСТВА ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА, В Т.Ч. СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ ТАЙНУ

2.1. Генеральный директор Общества, либо лицо, исполняющее его обязанности, является лицом, ответственным за обеспечение охраны информации ограниченного доступа, в том числе сведений, составляющих КТ, обладателями которой является Общество и его контрагенты, и осуществляет общее руководство работами по защите таких сведений и функционированию в Обществе режима конфиденциальности.

2.2. Генеральный директор Общества:

- утверждает перечень защищаемых информационных ресурсов Общества, в том числе перечень сведений, составляющих КТ и перечень защищаемых информационных ресурсов

информационных систем персональных данных Общества;

- своим решением назначает должностных лиц, ответственных за обеспечение режима конфиденциальности в Обществе;
- определяет состав комиссии, для разработки перечня сведений, составляющих коммерческую тайну Общества;
- определяет состав комиссии, осуществляющей проверку наличия документов с грифом конфиденциальности и иных материальных носителей информации ограниченного доступа, и принимающей решение об уничтожении таких документов и материальных носителей;
- по запросу руководителя структурного подразделения разрешает допуск работника к информации ограниченного доступа, в том числе к сведениям, составляющим КТ, либо принимает решение о прекращении допуска сотрудника к указанным сведениям;
- своим решением утверждает Положение о конфиденциальности информации и Инструкцию о порядке учета, хранения и обращения с носителями информации ограниченного доступа;
- принимает решение о проведении служебной проверки по выявленному факту нарушения режима конфиденциальности и о наказании лица, виновного в нарушении режима конфиденциальности, на основании материалов служебной проверки по факту такого нарушения;
- разрешает передачу сведений ограниченного доступа контрагентам и предоставление таких сведений органам власти и местного самоуправления, следствия, дознания и судопроизводства с целью выполнения требований законодательства Российской Федерации, при этом руководствуясь принципом обеспечения разумного баланса между открытостью деятельности Общества и стремлением обеспечить защиту его интересов;
- принимает решение о прекращении работ на участках, где выявлены нарушения в обеспечении безопасности сведений ограниченного доступа, а также о возобновлении выполнения работ после их устранения;
- принимает решение о финансировании мероприятий по защите сведений ограниченного доступа.

2.3. Непосредственное руководство работами по защите информации ограниченного доступа, и контроль за функционированием режима конфиденциальности в Обществе осуществляет заместитель генерального директора по общим вопросам, который:

- организует работу по защите информации ограниченного доступа, и функционированию режима конфиденциальности;
- определяет состав комплекса режимных мер по согласованию с генеральным директором Общества;
- участвует в разработке перечней защищаемых информационных ресурсов Общества;
- рассматривает информацию и отчеты о состоянии защиты информации в Обществе;
- является председателем комиссии, осуществляющей проверку наличия документов с грифом конфиденциальности и иных материальных носителей информации ограниченного доступа, и принимающей решение об уничтожении таких документов и материальных носителей;
- докладывает генеральному директору о выявленном факте нарушения режима конфиденциальности в Обществе для принятия решения о проведении служебной проверки;
- согласует проведение служебной проверки по фактам нарушения режима конфиденциальности в Обществе;
- организует проведение совещаний по вопросам информации ограниченного доступа, в том числе:

а) по доведению результатов проверок и мониторинга состояния защиты информации в Обществе;

б) по результатам служебных расследований и разбирательств по вопросам нарушения режима конфиденциальности;

- согласует с генеральным директором Общества, либо с иным уполномоченным лицом, бюджет, необходимый для обеспечения функционирования режима конфиденциальности;
- согласует допуск сотрудников к работам с информацией ограниченного доступа, в т.ч. со сведениями, составляющими КТ;

- представляет генеральному директору Общества информацию о выявленных нарушениях в обеспечении безопасности сведений ограниченного доступа, для принятия решения о прекращении работ на участках, где выявлены такие нарушения.

2.4. Реализация мероприятий по защите информации ограниченного доступа в Обществе осуществляются отделом информационных технологий. Ответственность за реализацию необходимого комплекса мероприятий по защите информации в Обществе, а также за реализацию функций и задач отдела, возлагаются на начальника отдела информационных технологий, который:

- участвует в разработке перечней защищаемых информационных ресурсов общества;
- согласует допуск сотрудников к работам с информацией ограниченного доступа, в т.ч. со сведениями, составляющими КТ;
- контролирует учет лиц, допущенных в установленном порядке к обработке сведений ограниченного доступа и учет материальных носителей информации ограниченного доступа;
- является членом комиссии, осуществляющей проверку наличия документов с грифом конфиденциальности и иных материальных носителей информации ограниченного доступа, и принимающей решение об уничтожении таких документов и материальных носителей;
- осуществляет мероприятия, направленные на обеспечение устойчивого функционирования режима конфиденциальности в Обществе, в том числе реализует технические меры по защите информации, при автоматизированной обработке сведений ограниченного доступа;
- при необходимости, инициирует внесение изменений во внутренние нормативные акты Общества для устранения выявленных нарушений и противоречий;
- обеспечивает своевременное предупреждение и реагирование на инциденты, представляющие угрозу для информационной безопасности Общества;
- информирует в установленном порядке ответственных должностных лиц Общества об угрозах и рисковых событиях информационной безопасности;

2.5. Отдел информационных технологий в рамках деятельности по обеспечению режима конфиденциальности в Обществе осуществляет следующие функции:

- учет лиц, допущенных в установленном порядке к обработке сведений ограниченного доступа и материальных носителей информации ограниченного доступа;
- регистрация, учет и размножение (копирование) документов с грифом конфиденциальности;
- регистрация и учет материальных носителей информации ограниченного доступа, в том числе сведений, составляющих коммерческую тайну;
- реализация технических мер по защите информации, при автоматизированной обработке сведений ограниченного доступа;
- осуществление мероприятий по обеспечению защиты информации ограниченного доступа, в т.ч. сведений, составляющих КТ Общества и сведений, в отношении которых Общество приняло на себя обязательства перед третьими лицами – обладателями информации по сохранению её конфиденциальности;
- предупреждение, и своевременное реагирование с целью предотвращения утечек информации ограниченного доступа, и других инцидентов, представляющих угрозу для информационной безопасности Общества;
- мониторинг состояния защиты информации ограниченного доступа в Обществе, и подготовка отчетов о состоянии режима конфиденциальности в Обществе;
- инструктаж работников, допущенных к обработке информации ограниченного доступа и разъяснение им положений локальных нормативных актов Общества, регламентирующих работу с указанной информацией.

2.6. Методологическое обеспечение и контроль за реализацией мероприятий по защите информации ограниченного доступа, в том числе сведений, составляющих КТ Общества, осуществляются отделом экономической безопасности. Ответственность за реализацию функций и задач отдела, возлагаются на начальника отдела экономической безопасности Общества, который:

- Участвует в разработке перечней защищаемых информационных ресурсов общества;
- является ответственным за поддержание Перечня сведений, составляющих коммерческую тайну, в актуальном состоянии, при необходимости, организует заседание комиссии для пересмотра Перечня и внесение в него изменений и дополнений;
- является лицом, ответственным за внесение изменений в настоящее Положение;
- является членом комиссии, осуществляющей проверку наличия документов с грифом конфиденциальности и иных материальных носителей информации ограниченного доступа, и принимающей решение об уничтожении таких документов и материальных носителей;
- при необходимости, инициирует внесение изменений во внутренние нормативные акты Общества для устранения выявленных нарушений и противоречий.

2.7. В рамках реализации режима конфиденциальности в Обществе отдел кадров выполняет следующие задачи:

- Ознакомление принимаемых на работу работников с локальными нормативными актами, регламентирующими поддержание режима конфиденциальности в Обществе;
- Включение в трудовые договора между Обществом и работниками, которым в связи с выполнением ими трудовых обязанностей необходим доступ к сведениям ограниченного доступа, в том числе составляющим КТ, специального раздела, предусматривающего обязательства работника о неразглашении доверенной ему информации ограниченного доступа;
- Проведение, по решению генерального директора, служебных проверок по фактам нарушения режима конфиденциальности Общества.

2.8. Руководители структурных подразделений Общества:

- участвуют в формировании и пересмотре перечня защищаемых информационных ресурсов общества;
- инициируют допуск сотрудников к обработке информации ограниченного доступа, необходимой им для выполнения своих должностных обязанностей;
- обеспечивают выполнение установленных в Обществе требований по организации обработки и защиты информации ограниченного доступа во вверенных им подразделениях.

2.9. Работник Общества, имеющий доступ к информации ограниченного доступа, в т.ч. сведениям, составляющим КТ, обязан:

- знать и выполнять требования локальных нормативных документов Общества по защите информации, знать перечни защищаемых информационных ресурсов;
- хранить в тайне известные ему сведения ограниченного доступа, информировать руководителя своего структурного подразделения и должностных лиц Общества, ответственных за обеспечение режима конфиденциальности, о фактах их разглашения или нарушения порядка обращения с носителями таких сведений, о попытках несанкционированного доступа к информации лиц, не имеющих на то права;
- пресекать действия других лиц, которые могут привести к нарушению конфиденциальности информации ограниченного доступа, в т.ч. к разглашению сведений, составляющих КТ;
- строго соблюдать правила пользования материальными носителями информации ограниченного доступа, порядок их учета и хранения, обеспечивать в процессе работы охрану конфиденциальности информации и предотвращать попытки доступа к ней посторонних лиц;
- знакомиться только с теми сведениями, к которым получен доступ в силу исполнения своих должностных обязанностей;
- немедленно сообщать своему непосредственному руководителю или лицу, его замещающему, об утрате или недостаче материальных носителей информации ограниченного доступа, в т.ч. материальных носителей информации, составляющей КТ, служебных пропусков, ключей от служебных помещений, сейфов, шкафов и рабочих столов, где хранятся носители информации ограниченного доступа, персональных идентификаторов, личных печатей и о других событиях, создающих предпосылки для несанкционированного доступа к информации ограниченного доступа;
- о допущенных нарушениях установленного порядка работы, учета и хранения

материальных носителей информации ограниченного доступа, в т.ч. материальных носителей сведений, составляющих КТ, а также о фактах разглашения таких сведений представлять письменные объяснения по требованию должностных лиц Общества, ответственных за обеспечение режима конфиденциальности, указанных в настоящем Положении;

- оказывать помощь и содействие при проведении внутренних служебных расследований по фактам нарушения режима конфиденциальности, попыток его нарушения или подготовки к нарушению;
- в случае установления виновности работника в разглашении информации ограниченного доступа, а именно сведений, составляющих КТ, возместить убытки, причиненные нарушением исключительного права Общества на секрет производства.

2.10. При прекращении или расторжении трудового, или гражданско-правового договора работник обязан:

- передать Обществу все имеющиеся у него носители информации ограниченного доступа, полученные и/или созданные им в рамках выполнения трудовых обязанностей и/или заданий Общества;
- не разглашать информацию ограниченного доступа, в т.ч. сведения, составляющие КТ, ставшие известными ему в период срока действия трудового (гражданско-правового) договора, до прекращения действия в отношении указанных сведений режима конфиденциальности в Обществе.

2.11. Работникам, имеющим доступ к информации ограниченного доступа, запрещается:

- передавать материальные носители сведений ограниченного доступа, без документального оформления факта передачи, а также передавать материальные носители сведений ограниченного доступа работникам Общества и иным лицам, не имеющим допуска к работе с такими сведениями, или знакомить их с такими сведениями в любой форме;
- передавать информацию ограниченного доступа в электронном виде, по незащищенным техническим каналам связи, без использования сертифицированных по требованиям безопасности информации ФСБ России средств криптографической защиты информации, принятых Обществом в эксплуатацию в установленном порядке, и согласования возможности такой передачи с отделом информационных технологий;
- использовать сведения, составляющие КТ, при осуществлении научной и педагогической деятельности, в открытой переписке, публикациях в СМИ, различного рода публичных выступлениях, а также в личных интересах;
- снимать копии с документов и других носителей сведений, составляющих КТ, или производить выписки из них на неучтенные носители, а равно использовать различные технические средства (фотоаппараты, видео и звукозаписывающую аппаратуру) для записи информации ограниченного доступа, без письменного разрешения руководителя подразделения, в котором был создан документ или иной материальный носитель информации ограниченного доступа, с соответствующим документальным оформлением;
- сохранять документы и иную информацию в электронном виде, на носители, не учтенные предварительно в установленном порядке в качестве материальных носителей сведений ограниченного доступа;
- выносить материальные носители информации ограниченного доступа, из зданий Общества, а также выполнять какие-либо работы, связанные с информацией ограниченного доступа, вне служебных помещений, без разрешения на то руководителя структурного подразделения;
- использовать сведения, ограниченного доступа, ставшие ему известными в ходе трудовой деятельности в Обществе, для занятия любыми иными видами деятельности;
- хранить личную информацию на корпоративных ресурсах (автоматизированные рабочие места, файловые хранилища и т.п.) и передавать ее по корпоративным каналам связи (корпоративная электронная почта, и др.).

3. ФОРМИРОВАНИЕ ПЕРЕЧНЯ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ ТАЙНУ

3.1. Определения и виды коммерчески значимой информации.

3.1.1. На основе определений, которые даются федеральным законодательством в отношении информации, составляющей коммерческую тайну, сформулированы её признаки (или критерии отбора информации). В общем случае сведения, составляющие КТ, – это информация, которая:

а) принадлежит Обществу на законном основании, не содержит сведений, являющихся собственностью государства (составляющих государственную или служебную тайну) и не является общедоступной;

б) отражает технологическую, торговую, финансовую и другие стороны деятельности Общества;

в) имеет действительную или потенциальную экономическую ценность, потребительную стоимость в силу неизвестности ее другим лицам, что дает возможность Обществу производить продукцию, товары или услуги, пользующиеся спросом на рынке, заключать равноправные, взаимовыгодные сделки с другими предприятиями, фирмами, находить новых клиентов, покупателей своей продукции;

г) может являться предметом посягательств других лиц (юридических или физических), так как к этой информации нет свободного доступа на законном основании;

д) охраняется Обществом, при этом Общество принимает надлежащие меры к охране ее конфиденциальности. Сохранение этой информации в тайне позволяет ей быть носителем коммерческой ценности.

3.1.2. К коммерческой тайне может быть отнесена научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в т.ч. составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой Обществом или ее обладателем введен режим ее защиты.

3.1.3. К коммерческой тайне также могут быть отнесены сведения, в отношении которых Общество обязано обеспечить реализацию необходимых мер защиты в соответствии с договорными или иными правовыми отношениями.

3.2. Критерии и методики отнесения информации к коммерческой тайне (КТ)

3.2.1. Для отнесения информации к коммерчески значимой дается её качественная и количественная оценка с точки зрения её реальной или потенциальной стоимости (ценности) по экономическим критериям. Ценность защищаемой коммерчески значимой информации объективно выражается разницей между прибылью, приносимой от её владения, и величиной затрат на защиту этой информации. Оценка по этим критериям носит приближенный характер, но позволяет провести дальнейшее уточнение – могут ли эти сведения являться коммерчески ценными и насколько они важны для Общества.

3.2.2. Решение о включении тех или иных данных о деятельности Общества в Перечень сведений, составляющих КТ определяется через анализ и учет возможных негативных последствий в случае их разглашения, к которым могут относиться:

- разрыв деловых отношений с партнерами;
- срыв переговоров, утрата возможности заключения выгодного контракта;
- снижение уровня сотрудничества с деловыми партнерами;
- невыполнение договорных обязательств;
- необходимость проведения дополнительных рыночных исследований;
- отказ от решений, ставших неэффективными в результате разглашения информации, и необходимость принятия дополнительных мер, связанных с финансовыми затратами;
- использование конкурентами полученных сведений для повышения экономического соперничества;
- потеря возможности патентования и продажи лицензий;

- сокращение конкурентами затрат на проведение НИОКР, совершенствование технологий,
- снижение цен на продукцию или снижение объемов продаж;
- нанесение ущерба авторитету Общества;
- снижение уровня экономической безопасности;
- опережение конкурентом вывода аналогичного товара на рынок;
- ухудшение условий получения кредитов;
- появление трудностей в снабжении, приобретении оборудования;
- увольнение ведущих специалистов Общества.

3.2.3. Чтобы избежать ошибок необоснованного отнесения сведений к КТ, специалистам Общества необходимо руководствоваться дополнительными критериями, отражающими преимущества отнесения информации к КТ. Наиболее общими из них являются:

- выигрыш во времени для Общества в сравнении с конкурирующими фирмами;
- уникальность разработки;
- новизна (новая функция потребления, новая технология, применение в новых областях);
- преимущество в технико-экономических характеристиках товара перед изделиями конкурентов;
- оригинальное применение материалов, технологий, преимущества в ценовой конкуренции, значительные трудозатраты для получения информации, монополия предприятия на информацию по данному направлению производственно-коммерческой деятельности;
- степень очевидности использования информации конкурентами в случае ее опубликования;
- появление возможности выхода на международные рынки, степень влияния на формирование у контрагентов положительного представления об Обществе;
- возможность обеспечения сохранности информации, в случае ее отнесения к КТ.

3.2.4. Можно выделить следующие основные группы сведений, по которым возможно отнесение сведения к КТ:

- Сведения стратегического характера: планы развития производства, в том числе с применением новых технологий, открытий и т.п.; причины, сдерживающие развитие предприятия, трудности и возможные пути их преодоления и т.п.
- Деловая информация: о торговых и деловых партнерах, клиентах, посредниках, поставщиках и т.д.; об условиях контрактов, соглашений, договоров и др.; о состоянии кредитно-финансовой системы Общества; планы реализации произведенной продукции; анализ конкурентоспособности; маркетинговая информация; планы рекламной деятельности и т.д.
- Технологическая и научно-техническая информация, лежащая в основе производства Обществом конкурентоспособной продукции: разработка технологий и новых видов продукции с учетом потребностей рынка; конструкция продукции; дизайн; формулы (физические, химические и тому подобное); методы производства; схемы и чертежи отдельных узлов, изделий и т.д.

3.3. Разработка перечня сведений, составляющих КТ

3.3.1. Разработка Перечня сведений, составляющих КТ (далее – Перечень КТ), является одним из основных мероприятий, направленных на формирование режима коммерческой тайны.

3.3.2. Перечень КТ формируется на основе анализа угроз экономической и технологической безопасности деятельности Общества на внешних и внутренних рынках судостроительной отрасли.

3.3.3. Разработка Перечня КТ осуществляется комиссией, назначаемой Генеральным директором Общества, в состав которой включаются руководители и сотрудники ведущих структурных подразделений Общества. В обязательном порядке в состав комиссии включаются сотрудники отдела ИТ.

3.3.4. К КТ не могут быть отнесены сведения, указанные в п. 4 ст. 8 Федерального Закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», ст. 5. ФЗ «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ, п. 11, ст. 13 Федерального закона «О бухгалтерском учёте» от 06.12.2011 №402-ФЗ, а также следующие категории сведений:

- сведения о чрезвычайных ситуациях, экологическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасности производственных объектов, безопасной деятельности работников Общества, а также безопасности граждан и населения в целом;
- сведения о порядке рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;
- сведения о решениях по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;
- сведения, необходимые для реализации прав, свобод и обязанностей работников.

3.3.5. Перечень КТ вступает в силу после утверждения его Генеральным директором Общества.

3.3.6. Пересмотр Перечня КТ и внесение в него изменений в случае изменения действующего законодательства Российской Федерации, регулирующего аспекты защиты сведений, составляющих КТ, а также нормативных актов Общества и Устава Общества, производится комиссией, состав которой приведен в п.3.3.3.

3.3.7. Ответственным за поддержание Перечня КТ в актуальном состоянии является начальник отдела экономической безопасности.

4. РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ С РАБОТНИКАМИ ПО ИСПОЛЬЗОВАНИЮ СВЕДЕНИЙ ОГРАНИЧЕННОГО ДОСТУПА, В ТОМ ЧИСЛЕ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ ТАЙНУ. ПОРЯДОК ДОСТУПА РАБОТНИКОВ К СВЕДЕНИЯМ, СОСТАВЛЯЮЩИМ КОММЕРЧЕСКУЮ ТАЙНУ

4.1. Общие положения.

4.1.1. Отношения Общества как работодателя с работниками, которым в связи с выполнением ими трудовых обязанностей необходим доступ к сведениям, ограниченного доступа, в т.ч. составляющим КТ, регулируются на основании трудового договора между Обществом и работником, в который включается специальный раздел, предусматривающий обязательства работника о неразглашении доверенной ему информации ограниченного доступа. В случае установления режима конфиденциальности, с работниками, имеющими на момент установления режима конфиденциальности трудовые договоры, заключаются соглашения о неразглашении информации ограниченного доступа, которые являются дополнением к трудовому договору и регулируют отношения Общества с работником в связи с установлением режима конфиденциальности.

В случае установления отношений с физическим лицом в форме гражданско-правового договора обязательства о конфиденциальности информации вводятся специальным разделом этого договора.

4.1.2. В трудовом договоре с Генеральным директором Общества должны предусматриваться его обязательства по обеспечению охраны конфиденциальности информации, обладателем которой является Общество и его контрагенты, и ответственность за обеспечение охраны ее конфиденциальности.

4.1.3. Исключительное право на секрет производства (предусмотренный статьей 1465 Гражданского кодекса Российской Федерации), созданный работником Общества в связи с выполнением своих трудовых обязанностей или конкретного задания, полученного от Общества, принадлежит Обществу.

Работник, которому в связи с выполнением своих трудовых обязанностей или конкретного задания Общества стал известен секрет производства, обязан сохранять конфиденциальность полученных сведений до прекращения действия исключительного права Общества на секрет производства, в том числе и после прекращения действия трудового договора.

4.1.4. Общество предоставляет работникам необходимые условия для выполнения требований по охране конфиденциальности информации ограниченного доступа, к которой

допускается работник: запираемые (а при необходимости – и опечатываемые) хранилища для документов, средства для доступа к информационным ресурсам коллективного пользования (ключи, пароли, индивидуальные идентификаторы и т.п.), обеспечивает контроль за доступом в помещения, где хранятся материальные носители информации ограниченного доступа, в том числе в нерабочее время, и принимает другие необходимые меры для обеспечения выполнения обязанностей, возложенных на работника в связи с доступом его к информации ограниченного доступа Общества и его контрагентов.

4.1.5. Общество вправе требовать охраны конфиденциальности информации ограниченного доступа Общества и/или его контрагентов, от лиц, получивших доступ к этой информации в результате действий, осуществленных случайно или по ошибке.

4.2. Порядок и условия доступа к информации ограниченного доступа, а также прекращения такого доступа:

4.2.1. К сведениям ограниченного доступа Общества, допускаются работники, которым такие сведения необходимы для выполнения их трудовых обязанностей, после заключения ими трудовых (гражданско-правовых) договоров или дополнительных соглашений к договору, закрепляющих обязательства работника по неразглашению информации ограниченного доступа, и ознакомления под подпись с перечнями защищаемых информационных ресурсов Общества, локальными нормативными актами, определяющими содержание режима конфиденциальности, и мерами ответственности за нарушение установленных режимных мер. Работу по ознакомлению работника с локальными нормативными актами, касающимися защиты информации в Обществе, и мерами ответственности за нарушение установленных режимных мер, выполняют работники Отдела кадров в процессе оформления трудовых отношений с работником.

Допуск к сведениям ограниченного доступа, осуществляет Генеральный директор Общества, либо лицо, которому делегированы права подписи трудовых договоров с работниками.

4.2.2. Работники Отдела информационных технологий проводят инструктаж (разъяснения) для лиц, которым необходим допуск к информации ограниченного доступа, об установленных мерах по защите информации в Обществе.

4.2.3. Отделом информационных технологий ведется учет лиц, имеющих допуск к информации ограниченного доступа, на основании данных, поступающих из Отдела кадров.

4.2.4. Доступ к сведениям ограниченного доступа, в полном объеме предоставляется Генеральному директору Общества и должностным лицам, ответственным за функционирование режима конфиденциальности в Обществе. Остальные работники допускаются только к тем сведениям (документам), которые необходимы им для выполнения возложенных на них обязанностей.

4.2.5. Обязанности работника Общества по соблюдению требований режима конфиденциальности и его ответственность за нарушение режимных мер отражаются в заключаемом с работником трудовом договоре или дополнительном соглашении к договору.

Примерный раздел трудового договора (дополнительного соглашения к трудовому договору) об обязательствах работника и руководителя по неразглашению информации ограниченного доступа приведен в Приложении 1 к настоящему Положению.

4.2.6. Доступ работников Общества к документам, содержащим сведения, ограниченного доступа, предоставляется на основании:

- письменной резолюции Генерального директора, либо должностного лица, исполняющего его обязанности, которая должна содержать: перечень фамилий работников, обязанных ознакомиться с документом или его исполнить, срок исполнения (при необходимости), другие указания, подпись руководителя и дату;
- распорядительных документов (приказов) о создании рабочих групп, комиссий по различным направлениям деятельности Общества, связанным со сведениями, составляющими КТ, в которых указываются должности и фамилии работников, а также конкретные поставленные задачи.

4.2.7. Доступ работников к информационным ресурсам Общества коллективного пользования (файловым серверам, приложениям, базам данных), содержащим сведения,

ограниченного доступа (далее – защищаемым информационным ресурсам), производится на основании заявки руководителя структурного подразделения работника, которому необходим доступ к защищаемым информационным ресурсам, на имя начальника отдела информационных технологий. В заявке указываются права, предоставляемые работнику в отношении информации ограниченного доступа, в т.ч. сведений, составляющих КТ Общества, в электронном виде (только чтение, чтение и редактирование и т.д.). Для предоставления доступа к ресурсам других структурных подразделений заявка должна быть согласована с владельцем требуемого ресурса. В случае несогласия владельца ресурса с допуском конкретного работника к ресурсу окончательное решение о допуске принимает Генеральный директор Общества.

После предоставления доступа пользователю в соответствии с заявкой работником отдела информационных технологий на заявке делается соответствующая запись.

Контроль за соблюдением установленной процедуры предоставления доступа возлагается на работника отдела информационных технологий, ответственного за обеспечение режима конфиденциальности, который должен иметь доступ к информации о правах пользователей корпоративной информационной системы в отношении защищаемых информационных ресурсов.

При наличии технической возможности заявки могут подаваться и согласовываться в электронном виде. Рекомендуется использовать технические средства контроля за соблюдением процедуры предоставления доступа к защищаемым информационным ресурсам и формирования отчетности о предоставленных правах доступа (средства управления идентификацией и доступом, управления информационной безопасностью и им подобные),

4.2.8. Учет движения документов, содержащих сведения, ограниченного доступа, и доступа к ним работников осуществляется по журналам приема-передачи документов, содержащих информацию ограниченного доступа, который ведется в структурных подразделениях, осуществляющих обработку информации ограниченного доступа, либо по журналам отдела информационных технологий.

4.2.9. Допуск работника к сведениям ограниченного доступа может быть прекращен в следующих случаях:

- расторжения трудового (гражданско-правового) договора (независимо от причин расторжения);
- нарушения работником условий договора или локальных нормативных актов Общества, связанных с неразглашением и обеспечением режима конфиденциальности;
- назначением работника на должность, не требующую доступа к информации ограниченного доступа, и/или изменения его трудовых обязанностей.

Прекращение допуска к информации ограниченного доступа осуществляется по решению Генерального директора Общества (или лица, выполняющего его обязанности), которое закрепляется в дополнительном соглашении к трудовому договору.

5. РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ С РАБОТНИКАМИ ПО ИСПОЛЬЗОВАНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Права, обязанности и ответственности работников, которым в связи с выполнением ими трудовых обязанностей необходим доступ к персональным данным, а также условия и порядок допуска регулируются «Положением об обработке персональных данных ПАО «ЦКБ «Айсберг», «Руководством пользователя информационных систем персональных данных «1С: Предприятие, модуль «1С: ERP зарплата (кадровый учет)», «АРМ пользователя №1», «Руководство администратора по обеспечению безопасности информации информационных систем персональных данных «1С: Предприятие, модуль «1С: ERP зарплата (кадровый учет)», «АРМ пользователя №1».

6. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ДЕЛОПРОИЗВОДСТВА

6.1. Принципы делопроизводства

6.1.1. Для установления порядка обращения с информацией ограниченного доступа, в т.ч.

со сведениями, составляющими КТ, с целью ограничения доступа к указанным сведениям используются следующие принципы:

- централизованный учет документов, содержащих сведения ограниченного доступа;
- учет лиц, получивших доступ к документам, содержащих сведения ограниченного доступа;
- обеспечение возможности использования сведений ограниченного доступа работниками и передачи ее контрагентам без нарушения режима конфиденциальности;
- запрет на ознакомление с информацией ограниченного доступа третьих лиц без согласия ее обладателя (Общества или его контрагента);
- организация доступа работников к документам, содержащим информацию ограниченного доступа, при использовании электронного документооборота, осуществляется на основе разрешительной системы доступа (матрицы доступа);
- при обработке сведений, составляющих КТ, разрешительная система доступа (матрица доступа) обеспечивает разграничение прав доступа не только к информационным ресурсам в целом, но и к конкретным документам в частности;
- система делопроизводства должна исключать несанкционированный доступ, утрату, подмену и/или хищение документов, содержащих сведения ограниченного доступа.

6.2. Основные требования к делопроизводству

6.2.1. Делопроизводство должно исключать несанкционированный доступ к документам, содержащим информацию ограниченного доступа, утрату, подмену или хищение таких документов, а также их случайное или умышленное уничтожение и удовлетворять следующим требованиям:

- централизованный учет документов, содержащих сведения ограниченного доступа; если характер сведений ограниченного доступа подразумевает простановку грифа конфиденциальности, простановка грифа осуществляется исполнителем или должностным лицом, подписывающим документ;
- при работе с документом должны соблюдаться условия, исключающие возможность ознакомления со сведениями ограниченного доступа посторонних лиц;
- размножение (копирование) документов, содержащих сведения ограниченного доступа, разрешается только по резолюции руководителя, в адрес которого направлен документ, либо который является инициатором создания такого документа;
- пересылка документа, содержащего информацию ограниченного доступа, обладателем которых является третья сторона, осуществляется только с письменного согласия обладателя указанных сведений, в т.ч. пересылка персональных данных работников Общества осуществляется с письменного согласия работников общества – субъектов персональных данных, на обработку персональных данных, включающую передачу таких персональных данных;
- с целью обеспечения контроля сохранности документов комиссией, в состав которой входят работники отдела информационных технологий, проводятся проверки наличия всех зарегистрированных документов с грифами конфиденциальности, наличие у исполнителей проектов документов, хранящихся в электронном виде, наличие всех учтенных машинных носителей, дел, журналов и правильность ведения всех видов учета;
- уничтожение документов и дел, содержащих сведения, ограниченного доступа утративших практическое значение, не имеющих научной или экономической ценности, срок хранения которых истек, производится с оформлением акта. После уничтожения носителей, содержащих сведения ограниченного доступа, в учетных документах (журналах, номенклатуре дел) проставляется отметка об уничтожении (порядок уничтожения носителей персональных данных определяется «Положением по обработке персональных данных ПАО «ЦКБ «Айсберг»);
- машинные носители информации для обработки сведений ограниченного доступа, подлежат учету. Использование личных (персональных) машинных носителей информации и ПЭВМ для обработки сведений ограниченного доступа, категорически запрещается.

6.3. Порядок оформления документов, содержащих сведения, ограниченного доступа

6.3.1. Оформление, учет, хранение и обращение с документами, содержащими сведения ограниченного доступа, в том числе сведения, составляющие КТ, осуществляется в порядке,

установленном «Инструкцией о порядке учета, хранения и обращения с носителями информации ограниченного доступа ПАО «ЦКБ «Айсберг».

6.3.2. Для проверки и контроля наличия документов с грифом конфиденциальности и иных материальных носителей информации ограниченного доступа, а также их уничтожения в связи с утратой практического значения и истечения срока хранения, решением генерального директора назначается состав комиссии, в которую входят работники отдела информационных технологий и отдела экономической безопасности.

6.3.3. Проверка наличия документов и их уничтожение, при необходимости, производятся ежегодно, в последний месяц года, либо в рамках проведения служебной проверки по факту выявленных нарушений при работе со сведениями ограниченного доступа в Обществе.

7. ОБЩИЕ ТРЕБОВАНИЯ К КОРПОРАТИВНЫМ ИНФОРМАЦИОННЫМ СИСТЕМАМ, В КОТОРЫХ ОСУЩЕСТВЛЯЕТСЯ ОБРАБОТКА ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА, В ТОМ ЧИСЛЕ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ ТАЙНУ

7.1. Технические (программные/аппаратно-программные) меры защиты в корпоративных информационных системах (КИС) Общества должны быть основаны на использовании в их составе аппаратного и программного обеспечения, реализующего (самостоятельно или в комплексе с другими средствами) функционал по защите информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, шифрование информации ограниченного доступа при передаче ее с использованием открытых каналов передачи данных, и т.п.).

7.2. С учетом принципов обеспечения информационной безопасности КИС, в которых осуществляется обработка информации ограниченного доступа, в состав системы защиты должны быть включены следующие средства:

- средства аутентификации пользователей КИС;
- средства разграничения доступа к данным;
- средства криптографической защиты информации при осуществлении информационного обмена информацией ограниченного доступа, с использованием открытых каналов передачи данных, в т.ч. информационно-телекоммуникационным сетям международного информационного обмена (сети Интернет);
- средства антивирусной защиты информации;
- средства межсетевого экранирования в целях отделения с локальной вычислительной сети Общества от информационно-телекоммуникационных сетей международного информационного обмена (сети Интернет).

8. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ ПРИ ВЫПОЛНЕНИИ ДОГОВОРНЫХ ОБЯЗАТЕЛЬСТВ ПЕРЕД СТОРОННИМИ ОРГАНИЗАЦИЯМИ И ПРИ ПРЕДОСТАВЛЕНИИ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ ТАЙНУ, ОРГАНАМ ГОСУДАРСТВЕННОЙ ВЛАСТИ И МЕСТНОГО САМОУПРАВЛЕНИЯ

8.1. Общие положения.

8.1.1. Отношения Общества с контрагентами, которым передаются сведения, составляющие КТ, регулируются гражданско-правыми договорами между Обществом и контрагентами.

8.1.2. Общество вправе требовать охраны конфиденциальности сведений, составляющих коммерческую тайну Общества и/или его контрагентов, от лиц, получивших доступ к этой информации в результате действий, осуществленных случайно или по ошибке.

8.2. Порядок и условия передачи контрагентам информации, составляющей коммерческую тайну Общества.

8.2.1. Передача контрагентам сведений, составляющих КТ, допускается только при наличии гражданско-правового договора между Обществом и контрагентом, существенным условием которого является охрана конфиденциальности передаваемой информации. В этих целях в договоре предусматривается специальный раздел о конфиденциальности.

8.2.2. Обязательства контрагента по обеспечению сохранности сведений, составляющих КТ, перед Обществом, передающим защищаемую информацию, также может закрепляться отдельным договором - Договором о конфиденциальности.

8.2.3. В случаях, если передаваемые сведения, составляющие КТ Общества, будет использоваться для извлечения контрагентом прибыли, между Обществом и контрагентом заключается один из следующих видов договоров[1]:

- договор об отчуждении исключительного права на секрет производства - в случаях, когда Общество передает все исключительные права на сведения, составляющие КТ, контрагенту без возможности использования Обществом передаваемой информации в дальнейшем;
- лицензионный договор о предоставлении права использования секрета производства - в случаях, когда контрагенту передаются неисключительные права использования секрета производства, а Общество продолжает или предполагает использовать его для извлечения прибыли, в том числе – заключения лицензионных договоров с другими контрагентами;
- договор коммерческой концессии – в случаях, когда неисключительные права использования секрета производства передаются контрагенту вместе с правами использовать комплекс принадлежащих Обществу исключительных прав, включающий право на товарный знак, знак обслуживания, а также права на другие предусмотренные договором объекты исключительных прав, такие, как коммерческое обозначение и т.п. Содержание раздела договора коммерческой концессии, определяющее порядок передачи и использования прав на секрет производства, аналогично лицензионному договору.

8.2.4. Ответственность за принятие решения о составе, объеме, порядке передачи и использования сведений, составляющих КТ, предоставляемых контрагенту, возлагается на лицо, подписавшее соответствующий гражданско-правовой договор.

Передача сведений, составляющих КТ, контрагентам в соответствии с заключенными договорами производится только на материальных носителях, на которые нанесен гриф «Коммерческая тайна» с указанием полного наименования Общества, его места нахождения и регистрацией факта передачи (отправки документов) в соответствующих формах учета (например, актов приема-передачи).

---

[1] Указанные в п. 8.2.3 виды гражданско-правовых договоров представлены исключительно в целях понимания различия между передачей информации, составляющей КТ, обладателем для оказания контрагентами работ (услуг) без извлечения прибыли, либо с извлечением таковой. Договоры об отчуждении исключительного права на секрет производства, лицензионный и коммерческой концессии не являются предметом детального рассмотрения в настоящем Положении.

Предоставление контрагенту сведений, составляющих КТ, на носителях, не имеющих грифа «Коммерческая тайна», а также направление документов, содержащих сведения, составляющие КТ, третьим лицам, с которыми не заключен соответствующий гражданско-правовой договор, запрещается.

При ознакомлении контрагента с документами, содержащими сведения, составляющие КТ, если контрагенту материальный носитель для дальнейшей работы не требуется, то регистрируется факт временной выдачи носителя (факт ознакомления контрагента с документами).

Материальные носители (документы), содержащие сведения, составляющие КТ, Общества, направляются контрагентам только с использованием специальной или фельдъегерской связи, а если такая возможность отсутствует – нарочным, курьерской службой или заказным письмом при обязательном подтверждении факта отправки письма квитанцией.

Направление контрагентам сведений, составляющих КТ, в электронном виде с использованием информационно-телекоммуникационных сетей общего пользования (Интернет) допускается только при условии использования сертифицированных по требованиям безопасности информации ФСБ России средств криптографической защиты информации, принятых Обществом и контрагентом в эксплуатацию в установленном порядке, а также наличия соглашения между Обществом и контрагентом о ведении электронного документооборота, в котором регулируются вопросы охраны конфиденциальности, подтверждения подлинности документов и неотказуемости от авторства.

Во всех остальных случаях использование незащищенных каналов связи для передачи информации КТ запрещается.

8.2.5. Переговоры, рабочие встречи, консультации, совещания (далее – переговоры) с контрагентами по вопросам, требующим ознакомления участников переговоров со сведениями, составляющими КТ Общества, проводятся только после заключения Обществом с участниками переговоров (контрагентами и/или физическими лицами) гражданско-правовых договоров, регулирующих охрану конфиденциальности КТ.

Результаты переговоров, на которых рассматривались сведения, составляющие КТ Общества, документируются и оформляются в виде протоколов, в которых указывается:

- полный состав участников от каждой из сторон переговоров с указанием фамилий, имен, отчеств и должностей, занимаемых участниками переговоров, наименований организаций, которые они представляют;
- краткое содержание обсуждаемых сведений с указанием номеров пунктов Перечня КТ, относящих данную информацию к КТ;
- факт ознакомления участников переговоров с мерами ответственности за разглашение (неправомерное использование) КТ Общества.

Протокол подписывается всеми участниками переговоров или лицами, уполномоченными контрагентами. В последнем случае эти лица оговариваются в тексте протокола. Один экземпляр протокола хранится в Обществе.

Пример типового договора о конфиденциальности и неразглашении информации приведен в Приложении 2 к настоящему Положению.

8.3. Предоставление информации, составляющей коммерческую тайну, органам государственной власти и местного самоуправления

8.3.1. Предоставление сведений, составляющих КТ, органам государственной власти, иным государственным органам, органам местного самоуправления (далее - органы власти) в целях выполнения ими своих функций, производится Обществом на безвозмездной основе по мотивированному требованию соответствующего органа власти. При этом мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правовое основание для затребования сведений, составляющих КТ, срок предоставления этой информации, если иное не установлено федеральными законами.

8.3.2. Запросы органов власти на предоставление сведений, составляющих КТ, принимаются только в письменном виде. Устные запросы на предоставление сведений,

составляющих КТ, - в том числе полученные по телефону, к рассмотрению не принимаются, о нем необходимо сообщить лицу, формулирующему запрос, и указать на наличие такой нормы в законодательстве о КТ. При получении запроса по электронной почте или в виде факсимильного сообщения необходимо убедиться, что адрес электронной почты или телефонный номер действительно принадлежит органу власти, направившему запрос, а должностное лицо, указанное в качестве инициатора запроса, действительно занимает соответствующую должность в данном органе власти.

8.3.3. После получения запроса необходимо удостовериться в том, что правообладателем запрашиваемой информации является Общество, запрашиваемая информация находится в ведении соответствующего органа власти, а возможность ее истребования предусмотрена законодательством.

Предоставление сведений, составляющих КТ, органам власти, в электронном виде с использованием средств связи общего пользования (в том числе по факсу) и информационно-телекоммуникационным сетям международного информационного обмена, запрещается. Все ответы на запросы, содержащие сведения, составляющие КТ Общества, направляются только в письменном виде специальной или фельдъегерской связью, а если такая возможность отсутствует - нарочным, курьерской службой или заказным письмом при обязательном подтверждении факта отправки письма квитанцией.

Исключения допускаются только в случае наличия с органами власти каналов связи, защищенных с использованием сертифицированных по требованиям безопасности информации ФСБ России средств криптографической защиты информации (например, предназначенных для сдачи налоговой, пенсионной и иной отчетности), организованных соответствующим органом власти, при наличии у Общества необходимых сертификатов соответствия, ключей шифрования и электронной подписи, необходимых программных средств и выполнении иных условий охраны конфиденциальности информации.

8.3.4. На всех материальных носителях, содержащих сведения, составляющие КТ, и предоставляемых по запросу органов власти, проставляется гриф «Коммерческая тайна» с указанием полного наименования Общества-обладателя исключительных прав на секрет производства и места его нахождения. Материальные носители сведений, составляющих КТ, подлежат предварительному учету в Обществе в соответствии с установленным для этого порядком.

Направление сведений, составляющих КТ, на носителях, не имеющих грифа «Коммерческая тайна», запрещается.

8.3.5. В ответе на запрос органа власти о предоставлении информации (сопроводительном письме) в обязательном порядке сообщается о наличии в предоставляемых материалах сведений, составляющих КТ Общества (с указанием наименований и иных реквизитов их носителей), а также делается напоминание о необходимости охраны конфиденциальности сведений.

8.3.6. Ответы на запросы органов власти о предоставлении сведений, составляющих КТ, Обществу, содержащие секреты производства, подписываются Генеральным директором Общества или лицом, его замещающим, заместителями генерального директора общества (в пределах их полномочий по распоряжению конкретными группами сведений), которые несут персональную ответственность за соответствие передачи информации интересам Общества и оценку законности ее истребования.

9. ОТВЕТСТВЕННОСТЬ

9.1. Разглашение информации ограниченного доступа, в т.ч. сведений, составляющих КТ, является чрезвычайным происшествием, и влечет за собой последствия, предусмотренные действующим законодательством, а также договорными обязательствами между Обществом и принятым на работу лицом.

В целях предотвращения разглашения информации ограниченного доступа и/или создания предпосылок к этому Общество оставляет за собой право, но не принимает каких-либо обязательств контролировать надлежащее использование работником технических средств обработки и

хранения информации, соблюдение им установленных режимных мер по охране конфиденциальности информации ограниченного доступа Общества и информации, в отношении которой Общество приняло на себя обязательства перед третьими лицами – обладателями информации по сохранению её конфиденциальности в том числе с использованием специализированных средств мониторинга.

Согласие работника с проведением контрольных мероприятий в отношении использования им средств хранения, обработки и передачи информации, закрепляется в трудовом (гражданско-правовом) договоре или дополнительном соглашении к нему. В случае несогласия работника с проведением указанных мероприятий, Общество вправе не предоставлять ему в пользование соответствующие технические средства.

9.2. По каждому факту разглашения информации ограниченного доступа, создания к этому предпосылок, или нарушения работником установленных режимных мер по охране конфиденциальности информации ограниченного доступа, проводится служебное разбирательство, выясняются все обстоятельства произошедшего инцидента, выявляются виновные в произошедшем лица (в том числе не создавшие необходимых условий для охраны конфиденциальности и не осуществившие контроль, предусмотренный локальными нормативными актами Общества), к виновным принимаются меры воздействия, а в систему охраны конфиденциальности вносятся улучшения, препятствующие возникновению подобных инцидентов в дальнейшем.

9.3. Ответственность за разглашение информации ограниченного доступа несет персонально каждый работник Общества, имеющий доступ к этим сведениям и допустивший их разглашение. В зависимости от величины ущерба, который нанесен Обществу в результате разглашения работником информации ограниченного доступа, в т.ч. сведений, составляющих КТ, а также наличия умысла в его действиях, виновное лицо может быть привлечено к дисциплинарной, гражданско-правовой, административной и уголовной ответственности.

9.4. Общество принимает решение о взыскании с виновных лиц убытков, нанесенных нарушением исключительного права на секрет производства, в порядке, предусмотренном действующим законодательством Российской Федерации.

9.5. При причинении работником, разгласившим сведения, составляющие КТ, убытков и при отказе добровольно возместить причиненный вред, Общество имеет право обратиться в суд в целях обеспечения защиты своих интересов.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. В случае изменения действующего законодательства и иных нормативных актов, содержащих требования к защите КТ, персональных данных и иной, охраняемой в соответствии с законодательством Российской Федерации, информации, настоящее Положение и изменения к нему применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также документам Общества.

10.2. Внесение изменений в настоящее Положение осуществляется, при необходимости, в следующих случаях:

- по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности,
- по результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий,
- изменений в действующем законодательстве.

10.3. Ответственным за внесение изменений в настоящее Положение является начальник отдела экономической безопасности.

ПРИЛОЖЕНИЕ 1
к «Положению о конфиденциальности
информации ПАО «ЦКБ «Айсберг»

Раздел трудового договора (дополнительного соглашения к трудовому договору) об обязательствах работника по неразглашению информации ограниченного доступа

1. Работник обязуется:

1.1. Не разглашать информацию ограниченного доступа Работодателя и информацию, в отношении которой Работодатель принял на себя обязательства перед третьими лицами – обладателями информации, по сохранению её конфиденциальности, переданную Работнику в ходе трудовой деятельности, которые ему будут доверены или станут известны в период действия настоящего договора.

1.2. Не сообщать устно или письменно кому бы то ни было информацию ограниченного доступа без соответствующего разрешения имеющих на то право лиц.

1.3. В случае попытки посторонних лиц получить информацию ограниченного доступа, немедленно сообщать об этом руководителю структурного подразделения, и работнику отдела информационных технологий, ответственному за обеспечение режима конфиденциальности.

1.4. Не использовать информацию ограниченного доступа для занятий любой деятельностью, которая в качестве конкурентного действия может нанести ущерб Работодателю.

1.5. При прекращении действия данного договора все материальные носители информации ограниченного доступа (документы, машинные носители, черновики, распечатки на принтерах и пр.), которые находились в его распоряжении в связи с выполнением должностных обязанностей, передать руководителю структурного подразделения, либо работнику отдела информационных технологий, ответственному за обеспечение режима конфиденциальности.

1.6. Об утрате или недостаче материальных носителей информации ограниченного доступа, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей и других фактах, которые могут привести к нарушению режима конфиденциальности, а также о причинах и условиях возможной утечки сведений ограниченного доступа, немедленно сообщать непосредственному руководителю, а также работнику отдела информационных технологий, ответственному за обеспечение режима конфиденциальности.

1.7. Использовать переданные ему Работодателем и установленные на рабочем месте технические средства обработки и передачи информации исключительно для выполнения обязанностей, предусмотренных настоящим договором.

2. Работодатель предоставляет Работнику необходимые условия для выполнения требований по защите конфиденциальности информации ограниченного доступа, к которой допускается Работник: хранилище для документов, средства для доступа к информационным ресурсам (ключи, пароли и т.п.) и др., определяемые обязанностями, выполняемыми Работником.

3. Работник разрешает (не препятствует) Работодателю производить контроль использования закрепленных за ним технических средств обработки и передачи информации в соответствии с регламентом, утвержденным работодателем, с которым он (работник) ознакомлен(а).

4. Работодатель оставляет за собой право, но не принимает каких-либо обязательств, контролировать надлежащие использование Работником технических средств обработки и хранения информации, соблюдение им мер по охране конфиденциальности, в том числе с использованием специализированных средств мониторинга.

5. Работник подтверждает, что не имеет никаких обязательств перед какими-либо физическими или юридическими лицами, которые входят в противоречие с настоящим договором, или которые ограничивают его трудовую деятельность в соответствии с настоящим договором.

6. Работодатель обязуется до начала выполнения должностных обязанностей Работником довести до его сведения соответствующие положения документов по защите информации ограниченного доступа, разглашение которой может нарушить данный договор.

7. Работник, которому, в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя, стал известен секрет производства, обязан сохранять конфиденциальность полученных сведений до прекращения действия исключительного права на секрет производства Работодателя или его контрагентов, которым секрет производства передан по договору об отчуждении исключительного права на секрет производства, в том числе и после прекращения действия трудового договора.

8. Работнику известно, что разглашение сведений ограниченного доступа, ставших ему известными в период действия настоящего договора, может повлечь дисциплинарную, административную, гражданско-правовую, уголовную ответственность, предусмотренную действующим законодательством Российской Федерации.

Раздел трудового договора с руководителем Общества, регулирующий отношения, связанные с коммерческой тайной

1. Генеральный директор (иное уполномоченное лицо) обязан обеспечить постоянный анализ результатов интеллектуальной деятельности работников с целью выявления информации, подлежащей правовой охране в режиме конфиденциальности (секретов производства), получения конкурентных преимуществ за счет использования такой информации, и обеспечения реализации исключительных прав Работодателя на такую информацию, и охраны ее конфиденциальности.

2. В случае выявления информации, имеющей действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, и отсутствия свободного доступа к ней на законном основании, установить в отношении такой информации режим конфиденциальности и с этой целью:

- определить порядок отнесения сведений к коммерческой тайне, организовать формирование перечня сведений, составляющих коммерческую тайну, и утвердить такой перечень;
- утвердить комплекс режимных мер, обеспечивающих охрану конфиденциальности секретов производства;
- утвердить порядок доступа к секретам производства работников и иных лиц, выполняющих в работы на основании гражданско-правовых и хозяйственных договоров;
- определить порядок передачи секретов производства контрагентам и предоставления их органам власти и местного самоуправления, следствия, дознания и судопроизводства с целью безусловного выполнения требований законодательства Российской Федераций, обеспечения разумного баланса между открытостью деятельности Работодателя и стремлением обеспечить защиту его интересов;
- организовать контроль за соблюдением установленных режимных мер, принятие мер воздействия к виновным в разглашении секретов производства и нарушении режимных мер, предотвращение инцидентов в дальнейшем.

3. Генеральный директор (или лицо, его замещающее) обязан обеспечить меры по охране конфиденциальности информации, обладателем которой являются контрагенты Работодателя, на уровне, соответствующем охране конфиденциальности собственных секретов производства и/или установленном договором с контрагентом.

4. Генеральному директору (или лицу, его замещающему) известно, что он может нести дисциплинарную, административную, уголовную ответственность, предусмотренную действующим законодательством Российской Федерации, в случае разглашения секретов производства Работодателя по его вине, вследствие его действия или бездействия, приведшего к разглашению информации или ее раскрытию вопреки интересам Работодателя, а также возместить убытки, нанесенные его виновными действиями в отношении охраны конфиденциальности информации, составляющей коммерческую тайну Работодателя.

ПРИЛОЖЕНИЕ 2
к «Положению о конфиденциальности
информации ПАО «ЦКБ «Айсберг»

Пример типового договора о конфиденциальности и неразглашении информации

Договор
о конфиденциальности и неразглашении информации

_____ "___" _____ 20__ г.
(место заключения)

Публичное акционерное общество «Центральное конструкторское бюро «Айсберг», именуемое в дальнейшем **«Передающая сторона»**, в лице _____, действующего на основании _____, с одной стороны, и _____, именуемое в дальнейшем **«Принимающая сторона»**, в лице _____, действующего на основании _____, с другой стороны, именуемые в дальнейшем **«Стороны»**, заключили настоящий договор, именуемый в дальнейшем «Договор», о нижеследующем:

1. Предмет Договора

1.1. Поскольку **Передающая сторона** является обладателем сведений, составляющей ее коммерческую тайну, а **Принимающая сторона** имеет намерение сотрудничать с **Передающей стороной** в рамках предполагаемых к заключению договоров, предметом настоящего Договора являются порядок, условия передачи **Передающей стороной**, получения и использования **Принимающей стороной** сведений, составляющих коммерческую тайну **Передающей стороны**.

1.2. Сведения, составляющие коммерческую тайну, фиксируются **Передающей стороной** на материальном носителе (в виде документа, массива данных на носителе информации для компьютеров или ином, по договоренности Сторон). На материальном носителе **Передающей стороной** проставляется гриф «Коммерческая тайна» с указанием полного наименования ее обладателя, места его нахождения и иных реквизитов, необходимых для идентификации носителя, что в совокупности является необходимым и достаточным условием для распространения на информацию, зафиксированную на таком носителе, условий настоящего Договора.

1.3. Содержание сведений, составляющих коммерческую тайну **Передающей стороны** и передаваемой **Принимающей стороне** в устной форме в ходе совещаний, переговоров, консультаций, рабочих встреч и т.п. (в дальнейшем именуемых «Совещание»), фиксируется в протоколе, который подписывается всеми участниками Совещания. Об обсуждении вопросов, с использованием сведений, составляющих коммерческую тайну, участники Совещания предупреждаются представителем **Передающей стороны** перед его началом, и ни один из участников не имеет права отказаться от подписания Протокола.

2. Передача сведений, составляющих коммерческую тайну:

Право принятия решения на передачу сведений, составляющих коммерческую тайну, принадлежит **Передающей стороне**.

3. Использование сведений, составляющих коммерческую тайну:

3.1. **Принимающая сторона** вправе использовать сведения, составляющие коммерческую тайну **Передающей стороны**, только для выполнения заключенных с **Передающей стороной** договоров об оказании услуг (выполнении работ, кредитования, проведения аудита и т.п. - оставить нужное).

Ни при каких обстоятельствах **Принимающая сторона** не может использовать полученные ей от **Передающей стороны** сведения, составляющие коммерческую тайну, для деятельности, направленной на извлечение прибыли, кроме как предусмотренной договорами с **Передающей стороной**.

3.2. **Принимающая сторона** обязуется принять все разумные и достаточные меры, чтобы не допустить несанкционированного доступа к сведениям, составляющим коммерческую тайну **Передающей стороны**, или ее передачи третьим лицам с нарушением условий настоящего Договора, а также организовать контроль за соблюдением этих мер.

3.3. Право раскрытия переданной информации, составляющей коммерческую тайну, и снятия грифа «Коммерческая тайна» с материальных носителей сведений, составляющих коммерческую тайну, принадлежит исключительно **Передающей стороне**.

3.4. **Принимающая сторона** обязана в минимально короткий срок с момента обнаружения признаков несанкционированного доступа третьих лиц к сведениям, составляющим коммерческую тайну **Передающей стороны**, уведомить об этом **Передающую сторону** и принять все возможные меры для уменьшения последствий несанкционированного доступа.

3.5. **Передающая сторона** соглашается и признает, что **Принимающая сторона** вправе

изготавливать достаточное количество копий материальных носителей сведений, составляющих коммерческую тайну, для лиц, указанных в пункте 3.6 настоящего Договора.

3.6. **Принимающая сторона** вправе сообщать сведения, составляющие коммерческую тайну **Передающей стороны**, своим работникам, имеющим непосредственное отношение к выполнению работ по договорам с **Передающей стороной** после подписания настоящего Договора, и в том объеме, в каком она им необходима для реализации условий договоров.

3.7. **Принимающая сторона** обязуется допускать к местам хранения, обработки и использования сведений, составляющих коммерческую тайну, **Передающую сторону**.

Передающая сторона в случае выявления нарушения требований охраны конфиденциальности сведений, составляющих ее коммерческую тайну, вправе запрещать или приостанавливать обработку таких сведений, а также требовать немедленного возврата или уничтожения полученных носителей сведений, составляющих коммерческую тайну.

Требования и указания **Передающей стороны**, касающиеся порядка охраны конфиденциальности сведений, составляющих ее коммерческую тайну, подлежат незамедлительному исполнению, если они изложены в письменном виде и вручены **Принимающей стороне**.

3.8. **Принимающая сторона** имеет право предоставлять сведения, составляющие коммерческую тайну **Передающей стороны**, третьим лицам в случаях, предусмотренных законодательством Российской Федерации. **Принимающая сторона** обязуется уведомлять **Передающую сторону** о каждом таком факте предоставления сведений, составляющих коммерческую тайну, а также об иных событиях, приведших к получению сведений, составляющих коммерческую тайну, представителями органов государственной власти, следствия и судопроизводства, в течение одного рабочего дня после наступления такого события.

Обязательства **Принимающей стороны** по обеспечению конфиденциальности не распространяются на сведения, полученные от передающей стороны в случаях если:

- они были известна на законном основании **Принимающей Стороне** до заключения настоящего Договора;
- они становятся публично известными в результате любых действий **Передающей стороны**, умышленных или неумышленных, а равно бездействия **Передающей стороны**;
- указанные сведения на законном основании получены **Принимающей стороной** от третьего лица без ограничений на их использование;
- указанные сведения получены из общедоступных источников с указанием на эти источники;
- указанные сведения раскрыты для неограниченного доступа третьей стороной.

3.9. В случае реорганизации или ликвидации одной из Сторон до даты прекращения действия настоящего Договора предусматривается следующий порядок охраны сведений, составляющих коммерческую тайну:

а) при реорганизации

- уведомление второй Стороны о факте реорганизации;
- возврат по требованию **Передающей стороны** или ее правопреемника сведений, составляющих коммерческую тайну **Передающей стороны**, на всех материальных носителях **Передающей стороне** или ее правопреемнику;

б) при ликвидации возврат сведений, составляющих коммерческую тайну, на всех носителях (в том числе изготовленных **Принимающей стороной** в соответствии с настоящим Договором) **Передающей стороне**.

3.10. **Принимающая сторона** обязана сохранять конфиденциальность сведений, составляющих коммерческую тайну **Передающей стороны**, до прекращения действия режима коммерческой тайны в отношении указанных сведений, в том числе в период после прекращения действия настоящего Договора.

4. Ответственность Сторон:

Принимающая сторона, допустившая разглашение сведений, составляющих коммерческую тайну **Передающей стороны**, или ее передачу (предоставление) третьим лицам с нарушением условий настоящего Договора, в том числе неумышленных, ошибочных действий или бездействия, несет ответственность в соответствии с законодательством Российской Федерации и обязана возместить убытки **Передающей стороны**.

5. Прочие условия:

5.1. Настоящий Договор вступает в силу с момента его подписания и действует в течение _____ лет с момента последней передачи сведений, составляющих коммерческую тайну.

5.2. Настоящий Договор подлежит юрисдикции и толкованию в соответствии с законами Российской Федерации.

5.3. Изменение условий настоящего Договора, его расторжение и прекращение допускаются по соглашению Сторон. Любые дополнения или изменения, вносимые в настоящий Договор, рассматриваются Сторонами, оформляются дополнительным соглашением и вступают в силу с даты его подписания Сторонами, если иное не будет указано в таком дополнительном соглашении.

5.4. Все споры, разногласия или требования, возникающие из настоящего Договора или в связи с ним, в том числе касающиеся его исполнения, нарушения, прекращения или недействительности, подлежат разрешению в арбитражном суде для разрешения экономических споров в соответствии с его регламентом.

5.5. Права и обязанности по настоящему Договору не подлежат переуступке третьим лицам без письменного согласия Сторон.

5.6. В случае изменения юридического адреса, расчетного счета или обслуживающего банка Стороны обязаны в десятидневный срок уведомить об этом друг друга.

5.7. Настоящий договор составлен и подписан в двух экземплярах, Имеющих равную силу - по одному для каждой из Сторон.

6. Реквизиты и подписи Сторон

Передающая сторона	**Принимающая сторона**
_____ / _____	_____ / _____
М.П.	М.П.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

В таблице приведены сведения о последних изменениях данного документа, включая версию, дату, автора и краткое описание изменений.

Версия	Дата	Автор	Изменения

ЛИСТ ОЗНАКОМЛЕНИЯ

№ п/п	Ф.И.О.	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				