

ОСК.СМК 00.202-2022

Приложение № 1

УТВЕРЖДЕНО

приказом АО «ОСК»

от «26» 10 2022 г. № 310

ПОЛОЖЕНИЕ

о коммерческой тайне АО «ОСК»

Санкт-Петербург

2022

Оглавление

I. Общие положения.....	3
II. Термины и определения	4
III. Порядок отнесения информации к коммерческой тайне и прекращения ограничения доступа к ней	6
IV. Маркировка.....	10
V. Обязанности ответственного в вопросах охраны конфиденциальности ИКТ ...	11
VI. Права Общества как обладателя ИКТ	13
VII. Регулирование отношений с работниками АО «ОСК»	14
VIII. Порядок допуска работников АО «ОСК» к информации, составляющей коммерческую тайну.....	15
IX. Прекращение допуска работников АО «ОСК» к ИКТ.....	16
X. Обязанности работников АО «ОСК», имеющих доступ к информации, составляющей коммерческую тайну	17
XI. Регулирование отношений, связанных с коммерческой тайной, с контрагентами и органами государственной власти.....	19
XII. Проведение переговоров с контрагентами по вопросам, требующим ознакомления участников с ИКТ	21
XIII. Предоставление ИКТ органам государственной власти	22
XIV. Особенности обращения с документами, содержащими информацию, составляющую коммерческую тайну	24
XV. Уничтожение материальных носителей ИКТ.....	25
XVI. Ежегодная проверка наличия материальных носителей информации, составляющей коммерческую тайну	26
XVII. Ответственность за нарушение порядка обращения с информацией, составляющей коммерческую тайну	27
XVIII. Заключительные положения.....	28
Приложение № 1	30
Приложение № 2	33
Приложение № 3	34
Приложение № 4.....	36
Приложение № 5.....	38

I. Общие положения

1.1. Настоящее Положение о коммерческой тайне АО «ОСК» (далее – Положение) разработано в соответствии с Федеральным законом от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и другими нормативными правовыми актами Российской Федерации, регулирующими отношения в области коммерческой тайны, охраны ее конфиденциальности, использования результатов интеллектуальной деятельности, а также локальными нормативными актами АО «ОСК» (далее – Общество).

1.2. Положение определяет порядок обращения с информацией, составляющей коммерческую тайну, и контроль за соблюдением такого порядка.

1.3. Положение распространяется на отношения, связанные с информацией, составляющей коммерческую тайну Общества и отнесенной к таковой в соответствии с Перечнем сведений, составляющих коммерческую тайну АО «ОСК» и методическими рекомендациями по его формированию и оценке коммерческой ценности (далее – Перечень ИКТ), а также на отношения, связанные с обработкой сведений, составляющих коммерческую тайну, которыми Общество обладает и/или которые переданы ему организациями и предприятиями различных форм собственности на условиях конфиденциальности, независимо от вида носителя, на котором они зафиксированы.

1.4. Положение не распространяется на информацию, содержащую сведения, составляющие государственную тайну, служебную тайну, служебную тайну в области обороны, а также на персональные данные.

1.5. Положение является документом, требования которого обязательны для выполнения всеми работниками Общества, прикомандированными лицами, а также лицами, работающими по гражданско-правовым договорам, заключенным с Обществом, взявшими на себя обязательство о сохранении коммерческой тайны и иной информации ограниченного доступа (приложение № 1).

1.6. Положение разработано с учетом учредительных документов АО «ОСК» в развитие Концепции информационной безопасности АО «ОСК» и уточняет ее положения в отношении защиты сведений, составляющих коммерческую тайну АО «ОСК».

1.7. Коммерческая тайна АО «ОСК» является собственностью Общества. Если она представляет собой результат совместной деятельности с другими организациями, основанной на договорных отношениях, то коммерческая тайна может быть собственностью двух и более сторон, что должно найти отражение в договоре между ними.

1.8. Для иных сведений конфиденциального характера по решению руководства АО «ОСК» может быть установлен особый порядок защиты, регламентируемый отдельными локальными нормативными актами.

II. Термины и определения

2.1. В настоящем Положении применяются следующие термины с соответствующими определениями:

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

информационные активы – информационные ресурсы или средства обработки информации Общества;

информация, составляющая коммерческую тайну Общества (ИКТ) – 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 Обществом введен режим коммерческой тайны;

исполнитель – лицо, создавшее документ, содержащий ИКТ, или принявшее решение о размещении сведений, составляющих коммерческую тайну, на материальном носителе;

коммерческая тайна – 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;

контрагент – сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

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

несанкционированный доступ к информации – доступ к информации, составляющей коммерческую тайну, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

носитель информации – материальный носитель (бумажный, электронный и другие) с зафиксированной на нем информацией, составляющей коммерческую тайну;

обладатель информации, составляющей коммерческую тайну – лицо (организация), которое владеет информацией, составляющей коммерческую тайну, на законном основании, имеет право ограничивать доступ к этой информации и устанавливать в отношении нее режим коммерческой тайны;

передача информации – 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;

предоставление информации – 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 – 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;

секрет производства (ноу-хау) – сведения любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность вследствие неизвестности их третьим лицам, если к таким сведениям у третьих лиц нет свободного доступа на законном основании и обладатель таких сведений принимает разумные меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны;

соглашение о конфиденциальности – юридический договор, заключенный сторонами с целью взаимного обмена материалами, знаниями или другой информацией с ограничением к ней доступа третьим лицам.

III. Порядок отнесения информации к коммерческой тайне и прекращения ограничения доступа к ней

3.1. Режим коммерческой тайны устанавливается в отношении сведений, содержащих производственную, техническую, экономическую, организационную и другую информацию, связанную с деятельностью АО «ОСК», не содержащих государственную тайну, служебную тайну, служебную тайну в области обороны, а также персональные данные.

3.2. Гриф «Коммерческая тайна» может быть проставлен на любых видах документов АО «ОСК» (приказы, распоряжения, исходящие письма, протоколы и т.д.). Документы с грифом «Коммерческая тайна» на бумажных носителях регистрируются ДУД в журнале согласно приложению № 2.

3.3. Сведения, составляющие коммерческую тайну, должны отвечать следующим требованиям:

3.3.1. Иметь действительную или потенциальную ценность для Общества.

3.3.2. Не являться общеизвестными или общедоступными.

3.3.3. Разглашение или утечка таких сведений может нанести ущерб Обществу.

3.4. Не может быть установлен режим коммерческой тайны в отношении сведений:

3.4.1. Содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах в соответствующие государственные реестры.

3.4.2. Содержащихся в документах, дающих право на осуществление предпринимательской деятельности.

3.4.3. О состоянии 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 населения в целом.

3.4.4. 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.

3.4.5. О задолженности работодателя по выплате заработной платы и по иным социальным выплатам.

3.4.6. О нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений.

3.4.7. О перечне лиц, имеющих право действовать без доверенности от имени юридического лица.

3.4.8. Обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена федеральными законами.

3.5. Отнесение сведений к коммерческой тайне АО «ОСК» осуществляется в соответствии с Перечнем ИКТ, утвержденным приказом Общества.

3.6. Перечень сведений разрабатывается Департаментом безопасности с учетом законодательства Российской Федерации путем экспертных оценок, на основании предложений структурных подразделений Общества, в соответствии с принципами обоснованности, законности и своевременности.

3.7. Обоснованность заключается в установлении путем экспертной оценки целесообразности скрывания конкретных сведений, вероятных экономических и иных последствий этого действия, исходя из баланса жизненно важных интересов Общества.

3.8. Законность заключается в соответствии скрываемых сведений положениям нормативных правовых актов Российской Федерации.

3.9. Предложения об изменениях и дополнениях в Перечень ИКТ принимаются Департаментом безопасности и утверждаются приказом АО «ОСК». Работники АО «ОСК» должны быть ознакомлены с Перечень ИКТ, а также изменениями и дополнениями, внесенными в него.

3.10. При принятии решения об отнесении информации к коммерческой тайне АО «ОСК» необходимо учитывать:

3.10.1. Не составляет ли она государственную тайну, служебную тайну, служебную тайну в области обороны или персональные данные.

3.10.2. Не входит ли она в перечень сведений, которые не могут составлять коммерческую тайну.

3.10.3. Не является ли она общеизвестной или общедоступной.

3.10.4. Преимущества открытого использования рассматриваемой информации по сравнению с ее скрытым использованием.

3.11. Содержание и состав ИКТ, а также сроки ограничений на доступ к ней или условия прекращения ограничений на доступ определяются Перечнем ИКТ.

3.12. Секреты производства (ноу-хау), на которые Общество имеет исключительное право, защищаются в режиме коммерческой тайны. Особенности обеспечения конфиденциальности секретов производства, в том числе при передаче прав на них контрагентам, устанавливаются Регламентом по защите секретов производства (ноу-хау) в АО «ОСК».

3.13. Общество не вправе установить режим коммерческой тайны в отношении сведений, законным обладателем которых является дочернее или

зависимое общество. В то же время обобщенные в рамках уставной деятельности Общества сведения о деятельности дочерних и зависимых обществ, при наличии у них действительной или потенциальной коммерческой ценности и неизвестности третьим лицам, на законном основании могут быть отнесены к коммерческой тайне Общества.

3.14. Целесообразность отнесения информации, содержащейся на материальном носителе (изложенной в документе), к коммерческой тайне определяет исполнитель по согласованию со своим руководителем. Персональную ответственность за отнесение или неотнесение конкретных сведений к коммерческой тайне Общества и проставление грифа «Коммерческая тайна» на ее носителе несут исполнитель и лицо, подписавшее (утвердившее) соответствующий документ, а в отношении договоров – работник ответственный за подготовку договора.

3.15. Само по себе включение той или иной категории сведений в Перечень ИКТ не может являться основанием для обязательного отнесения соответствующей информации к коммерческой тайне. При определении возможности, необходимости и целесообразности отнесения тех или иных сведений к коммерческой тайне исполнитель, помимо Перечня ИКТ, исходит из оценки содержания конкретной информации и особенностей ее обращения, учитывая в частности следующие факторы и условия:

3.15.1. Коммерческую ценность информации и наличие к ней потенциального интереса третьих лиц.

3.15.2. Важность сведений с точки зрения получения прибыли в условиях конкуренции с другими субъектами рынка.

3.15.3. Возможность использования сведений конкурентами в случае их получения, в том числе в формах недобросовестной конкуренции, а также возможные последствия такого использования для Общества.

3.15.4. Возможность использования информации в бизнес-процессах в условиях ограничения доступа к ней и введения режимных мер.

3.15.5. Временной интервал (срок коммерческой значимости ИКТ), в течение которого информация является потенциально коммерчески ценной и финансово значимой для третьих лиц, что делает актуальными угрозы утечки ИКТ для ее обладателя.

3.15.6. Наличие других факторов и условий, которые могут представлять угрозу экономическим интересам Общества.

3.16. В случае если та или иная категория информации не включена в Перечень ИКТ, однако, по мнению исполнителя и/или его руководителя, обладает признаками ИКТ, на носитель(и) такой информации проставляется гриф

«Коммерческая тайна», а на имя директора Департамента безопасности подается служебная записка с предложением о внесении изменений в Перечень ИКТ (дополнение и/или изменение, прекращение отнесения информации к ИКТ), согласованная с директором Департамента правового обеспечения и директором Департамента имущественных прав. Полученные предложения анализируются работниками Департамента безопасности и передаются на утверждение генеральному директору АО «ОСК».

3.17. Прекращение отнесения сведений к коммерческой тайне осуществляется при утрате этими сведениями действительной или потенциальной коммерческой ценности в силу неизвестности ее третьим лицам, при наступлении событий, в результате которых знание указанных сведений третьими лицами не может причинить Обществу экономического ущерба, их раскрытие становится обязательным в соответствии с законодательством Российской Федерации, а также при государственной регистрации (патентовании) секретов производства (ноу-хау), охранявшихся до этого в режиме коммерческой тайны.

3.18. Прекращение действия режима коммерческой тайны в отношении сведений, ранее отнесенных к коммерческой тайне, осуществляется генеральным директором (лицом, его замещающим) Общества единолично или на основании заключения о необходимости прекращения действия режима коммерческой тайны, подготовленного структурным подразделением, в зоне ответственности (компетенции) которого находилась данная информация. В заключении отражаются основания утраты ценности информации и приводится обоснование отсутствия ущерба Обществу при отмене в отношении информации режима коммерческой тайны.

3.19. Факт несанкционированного получения ИКТ лицами, не имеющими на то законного права, в том числе в устной форме, не может служить безусловным основанием для прекращения отнесения информации к коммерческой тайне. Решение должно приниматься с учетом оценки возможности сохранения конфиденциальности таких сведений, в том числе лицом, получившим такие сведения в результате ошибки или случайности, а также полноты соответствия разглашенных сведений охраняемым.

3.20. В случае принятия решения о прекращении действия режима коммерческой тайны в отношении сведений необходимо:

3.20.1. Снять документ с учета с оформлением акта.

3.20.2. Удалить гриф с носителей информации (перечеркнуть одной чертой), под грифом указать реквизиты акта о снятии документа с учета.

3.20.3. Прекратить в отношении документов, снятых с учета, действие ограничений, применяемых для ИКТ.

3.20.4. Направить контрагентам (при наличии таковых) извещение о прекращении действия режима коммерческой тайны в отношении ранее направленных документов с указанием реквизитов акта о снятии их с учета.

IV. Маркировка

4.1. На все материальные носители, содержащие ИКТ (бумажные, машинные носители информации, CD/DVD и другие), проставляется гриф «Коммерческая тайна» с указанием полного наименования и местонахождения Общества (юридического адреса).

4.2. В случае если на одном материальном носителе содержатся сведения, относящиеся к служебной тайне в области обороны, и ИКТ, на нем проставляется ограничительная пометка «Для служебного пользования» с указанием пункта Перечня сведений Вооруженных Сил Российской Федерации, подлежащих отнесению к служебной тайне в области обороны, утвержденного приказом Министра обороны Российской Федерации от 17 января 2022 г. № 22.

4.3. Гриф с указанием полного наименования и местонахождения Общества (юридического адреса) печатается на документах без кавычек в правом верхнем углу первого листа шрифтом 11 размера, ограничивается правым полем и не подчеркивается. Гриф дополняется номером экземпляра, который проставляется через одинарный межстрочный интервал и центрируется по отношению к нему, но не подчеркивается:

Коммерческая тайна
Акционерное общество
«Объединенная судостроительная
корпорация»
191119, Санкт-Петербург,
ул. Марата, д. 90
Экз. № __

4.4. Кроме указанных реквизитов документа на оборотной стороне последнего листа каждого экземпляра в соответствии с Инструкцией по делопроизводству в АО «ОСК» печатается расчет рассылки.

4.5. При использовании или создании электронных документов, содержащих ИКТ, гриф «Коммерческая тайна» наносится в колонтитуле в системе электронного документооборота, используемой в Обществе.

V. Обязанности ответственного в вопросах охраны конфиденциальности ИКТ

5.1. Должностным лицом Общества, уполномоченным в вопросах охраны конфиденциальности ИКТ, является директор Департамента безопасности, на которого возлагается:

5.1.1. Руководство работами по установлению и изменению режима коммерческой тайны, организация режимных мероприятий, определение порядка обращения с ИКТ, организация разработки проектов локальных нормативных актов Общества по этим вопросам:

в части требований к построению, изложению, оформлению и содержанию документов Общества, определяющих действия и порядок признания и защиты исключительных прав на секреты производства (ноу-хау), – совместно с отделом управления интеллектуальной собственностью;

в части оценки ИКТ, стоимости прав на ноу-хау – совместно с Департаментом экономики;

в части технических средств защиты информации – совместно с Департаментом цифровой трансформации и информационных технологий (далее – ДЦТиИТ).

5.1.2. Координация, в рамках компетенции и зоны ответственности, установленных в соответствии с Положением о Департаменте безопасности, работы структурных подразделений Общества в вопросах защиты ИКТ, осуществление контактов с правоохранительными органами, государственными регуляторными и надзорными органами по вопросам, связанным с защитой ИКТ, подразделениями безопасности и защиты информации федеральных органов исполнительной власти.

5.1.3. Организация разработки и реализации практических мер по защите ИКТ Общества при ее обработке и передаче с использованием технических средств.

5.1.4. Проведение проверки совместно с Департаментом управления персоналом (далее – ДУП) принимаемых на работу лиц, организация их инструктажа по вопросам защиты коммерческой тайны.

5.1.5. Разработка и осуществление мер по предупреждению разглашения ИКТ при обмене информацией с заказчиками, партнерами и иными организациями.

5.1.6. Организация обучения совместно с ДУП работников Общества порядку и правилам обращения с ИКТ, проведение мероприятий по повышению осведомленности в вопросах обеспечения конфиденциальности ИКТ.

5.1.7. Осуществление контроля совместно с ДЦТиИТ, ДУП и Управлением внутреннего контроля и управления рисками за соблюдением требований по охране конфиденциальности ИКТ, проведение периодических проверок на предмет выполнения требований Положения.

5.1.8. Контроль порядка подготовки информационных материалов для размещения в средствах массовой информации – совместно с Департаментом взаимодействия с органами государственной власти и связям с общественностью на предмет разглашения информации, составляющей коммерческую тайну.

5.1.9. Организация расследования инцидентов, связанных с утечками, разглашением, несанкционированной передачей или распространением ИКТ, безотносительно того, был ли такой инцидент обусловлен умыслом, произошел случайно или в результате ошибки.

5.2. Для выполнения своих функций директор Департамента безопасности имеет право:

5.2.1. Выносить на рассмотрение руководства Общества вопросы, касающиеся реализации и изменения мер режима коммерческой тайны.

5.2.2. Требовать от всех работников Общества соблюдения режима коммерческой тайны.

5.2.3. Организовывать работы по оценке (силами работников Общества или с привлечением внешних специалистов и организаций, в том числе на договорной основе) достаточности принятых в Обществе мер по обеспечению безопасности информационных ресурсов.

5.2.4. Привлекать по согласованию с руководителями структурных подразделений Общества отдельных специалистов к подготовке проектов локальных нормативных актов Общества по обеспечению безопасности ИКТ.

5.2.5. Проводить проверки соблюдения в структурных подразделениях Общества требований локальных нормативных актов Общества в части обеспечения режима коммерческой тайны.

5.2.6. Инициировать представления руководству Общества по отстранению от работы с ИКТ работников Общества, нарушающих установленные требования по обращению с ней, и запрещению обработки информации техническими средствами, не обеспечивающими их защиту.

5.2.7. Требовать предоставления от работников Общества дополнительной информации, свидетельств, любых данных и сведений, необходимых для проведения расследований инцидентов, связанных с утечками, разглашением, несанкционированной передачей или распространением ИКТ, безотносительно того, был ли такой инцидент обусловлен умыслом, произошел случайно или в результате ошибки.

5.2.8. Передавать сведения о фактах разглашения ИКТ, а также материалы проведенных расследований в компетентные государственные органы.

VI. Права Общества как обладателя ИКТ

6.1. Обладателем информации, составляющей коммерческую тайну АО «ОСК», полученной работниками Общества в рамках трудовых отношений, является работодатель, то есть АО «ОСК». Все работники Общества используют такую информацию только во время своей работы, но не обладают ею персонально, хотя могут корректировать ее содержание или наращивать ее объемы.

6.2. Общество как обладатель информации, отнесенной им к коммерческой тайне, имеет право:

6.2.1. Устанавливать, изменять и отменять в письменной форме режим коммерческой тайны как в целом в Обществе, так и в отношении конкретных сведений (групп сведений).

6.2.2. Использовать ИКТ для собственных нужд и по собственному усмотрению любым способом, не противоречащим законодательству Российской Федерации.

6.2.3. Разрешать или запрещать доступ к ИКТ.

6.2.4. Определять порядок и условия доступа к ИКТ.

6.2.5. Принимать решение о раскрытии ИКТ контрагентам на основании заключенных Соглашений о конфиденциальности (пункт 11.4 настоящего Положения).

6.2.6. Требовать соблюдения обязанностей по охране ИКТ от юридических и физических лиц, получивших доступ к такой информации на основании заключенных Соглашений о конфиденциальности (пункт 11.4 настоящего Положения), от органов государственной власти, иных государственных органов, которым предоставлена ИКТ.

6.2.7. Защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами ИКТ, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

6.3. Наряду с организационными мерами обеспечения конфиденциальности информации в АО «ОСК» применяются средства и методы технической защиты конфиденциальной информации, а также другие меры, не противоречащие законодательству Российской Федерации.

6.4. При реорганизации Общества (в форме слияния, присоединения, разделения, выделения или преобразования) право на установление, изменение или отмену режима коммерческой тайны переходит к его правопреемнику.

6.5. При ликвидации Общества ликвидационная комиссия принимает решение о порядке использования имеющейся в его распоряжении ИКТ.

VII. Регулирование отношений с работниками АО «ОСК»

7.1. Отнесение информации к сведениям, составляющим коммерческую тайну АО «ОСК», не исключает возможность общения между работниками Общества в отношении такой информации, если это входит в круг их должностных обязанностей.

7.2. Отношения Общества с работниками АО «ОСК», которым в связи с выполнением ими трудовых обязанностей необходим доступ к ИКТ, регулируются на основании трудовых договоров между Обществом как работодателем и работниками, в которые включается специальный раздел, предусматривающий обязательства работника о сохранении доверенной ему ИКТ, либо оформляются отдельным документом – обязательством о сохранении коммерческой тайны и иной информации ограниченного доступа. В случае установления (изменения) режима коммерческой тайны в Обществе с работниками АО «ОСК», имеющими на момент установления (изменения) режима коммерческой тайны трудовые договоры, заключаются обязательства о сохранении коммерческой тайны и иной информации ограниченного доступа, которые являются дополнительными соглашениями к трудовым договорам и регулируют отношения работодателя с работниками по использованию ИКТ.

7.3. Работники Общества допускаются к работе с ИКТ только после ознакомления с настоящим Положением и подписания обязательства о сохранении коммерческой тайны и иной информации ограниченного доступа.

7.4. В случае оказания физическими лицами услуг Обществу (выполнение работ для Общества) на основании гражданско-правовых договоров обязательства о сохранении коммерческой тайны и иной информации ограниченного доступа Общества и его контрагентов устанавливаются специальным разделом такого договора либо путем подписания Соглашения о конфиденциальности (пункт 11.4 настоящего Положения).

7.5. С членами совета директоров и иных органов управления юридических лиц, входящих в одну группу компаний с Обществом, принимающими решения по вопросам деятельности Общества, но не являющимися работниками Общества, заключаются Соглашения о конфиденциальности (пункт 11.4 настоящего Положения).

7.6. Гражданин, в том числе работник Общества или бывший его работник, которому в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя стала известна ИКТ, обязан сохранять конфиденциальность полученных сведений в течение всего срока действия режима коммерческой тайны в отношении этих сведений.

7.7. Общество предоставляет работникам необходимые условия для выполнения требований по охране коммерческой тайны Общества, к которой допускаются работники: предоставляет запираемые хранилища (шкафы) для документов, средства для доступа к информационным ресурсам коллективного пользования (ключи, пароли, индивидуальные идентификаторы и т.п.), доступ к электронным документам, размещенным на защищаемых информационных ресурсах, обеспечивает контроль за доступом в помещения, где хранятся материальные носители коммерческой тайны, в том числе в нерабочее время, и принимает другие необходимые меры для обеспечения выполнения обязанностей, возложенных на работников АО «ОСК» в связи с доступом их к коммерческой тайне Общества.

VIII. Порядок допуска работников АО «ОСК» к ИКТ

8.1. К ИКТ допускаются работники АО «ОСК», которым такие сведения необходимы для выполнения их трудовых обязанностей, после заключения с ними трудовых (гражданско-правовых) договоров или дополнительных соглашений к договорам, закрепляющих обязательства работника по неразглашению ИКТ, и ознакомления под подпись с Перечнем ИКТ и настоящим Положением. Ознакомление работника с локальными нормативными актами, определяющими режим коммерческой тайны, и мерами ответственности за нарушение установленных режимных мер выполняют работники Департамента управления персоналом при оформлении (изменении) трудовых отношений с работником АО «ОСК» или изменении его трудовых обязанностей, предусматривающих доступ к ИКТ.

8.2. Допуск к ИКТ осуществляет генеральный директор Общества либо лицо, которому им делегированы права подписи трудовых договоров с работниками Общества.

8.3. Работники Департамента безопасности при необходимости проводят инструктаж (разъяснение) с лицами, которым необходим доступ к ИКТ, об установленных АО «ОСК» мерах по защите ИКТ.

8.4. Доступ к ИКТ предоставляется членам совета директоров и иных органов управления юридических лиц, входящих в одну группу компаний с Обществом, принимающих решения по вопросам деятельности Общества, в объеме, необходимом для принятия соответствующих решений. Доступ к ИКТ в полном объеме предоставляется генеральному директору Общества, заместителям генерального директора, директорам Департамента безопасности и Департамента правового обеспечения, Департамента управления делами. Остальные работники

АО «ОСК» допускаются только к тем сведениям (документам), которые необходимы им для выполнения возложенных на них обязанностей.

8.5. Доступ работников Общества к документам, содержащим ИКТ, предоставляется на основании:

8.5.1. Настоящего Положения, утвержденного приказом Общества.

8.5.2. Оформленного в установленном порядке обязательства о сохранении коммерческой тайны и иной информации ограниченного доступа (дополнительного соглашения к трудовому договору).

8.5.3. Письменной или оформленной в системе электронного документооборота резолюции генерального директора Общества или руководителя структурного подразделения Общества, к компетенции которого относится ИКТ, на носителе ИКТ или сопроводительном письме к нему, которая должна содержать: перечень фамилий работников, обязанных ознакомиться с документом или его исполнить, срок исполнения, другие указания, подпись руководителя и дату. При этом все лица, кроме генерального директора (лица, его замещающего), могут предоставлять доступ к ИКТ только подчиненным им работникам.

8.5.4. Организационно-распорядительных документов (приказов) Общества о создании рабочих групп, комиссий и т.д., деятельность которых связана с ИКТ, где указываются должности и фамилии работников АО «ОСК», а также конкретные поставленные задачи.

8.5.5. Должностных инструкций работников (только для работников Аппарата председателя совета директоров, Аппарата генерального директора, Департамента безопасности, Департамента правового обеспечения, работающих с ИКТ на постоянной основе, а также администраторов ИТ-систем, на которых возложена обязанность предоставления доступа к информационным ресурсам, на которых хранится и обрабатывается ИКТ).

8.6. В системе электронного документооборота реализован разделенный доступ к файлам (документам), содержащим ИКТ, и обеспечивается их маркировка (нанесение грифа «Коммерческая тайна»).

8.7. Учет доступа работников и иных лиц к информационным ресурсам, где хранится и обрабатывается ИКТ, автоматически ведется в электронных журналах событий (сообщений) (логов) операционной системы, приложений и систем управления базами данных.

IX. Прекращение допуска работников АО «ОСК» к ИКТ

9.1. Допуск работника АО «ОСК» к ИКТ может быть прекращен в случаях:

9.1.1. Расторжения трудового (гражданско-правового) договора (независимо от причин расторжения).

9.1.2. Нарушения работником условий договора или локальных нормативных актов Общества, связанных с неразглашением и обеспечением конфиденциальности ИКТ.

9.1.3. Назначения работника на должность, не требующую доступа к ИКТ, и/или изменения его трудовых обязанностей.

9.2. Прекращение допуска работника к ИКТ осуществляется по решению работодателя, которое закрепляется в дополнительном соглашении к трудовому договору.

Х. Обязанности работников АО «ОСК», имеющих доступ к ИКТ

10.1. Работник Общества, имеющий доступ к ИКТ, обязан:

10.1.1. Знать и выполнять требования настоящего Положения, локальных нормативных актов Общества, определяющих режим защиты ИКТ и иной конфиденциальной информации, знать Перечень ИКТ.

10.1.2. Хранить в тайне ИКТ, в том числе тех организаций, с которыми имеются договорные отношения у Общества, информировать руководителя своего структурного подразделения и Департамент безопасности о фактах разглашения ИКТ или нарушения порядка обращения с носителями таких сведений, о попытках несанкционированного доступа к информации лиц, не имеющих на то права.

10.1.3. Пресекать действия других лиц, которые могут привести к разглашению ИКТ.

10.1.4. Соблюдать правила пользования материальными носителями ИКТ, порядок их учета и хранения, обеспечивать в процессе работы охрану ИКТ и предотвращать попытки доступа к ней посторонних лиц.

10.1.5. Знакомиться только с теми сведениями, к которым получен доступ в силу исполнения своих должностных обязанностей.

10.1.6. Немедленно сообщать своему непосредственному руководителю, а также в Департамент безопасности об утрате или недостатке материальных носителей ИКТ, служебных пропусков, ключей от служебных помещений, сейфов, шкафов и рабочих столов, где хранятся носители ИКТ, персональных идентификаторов, личных печатей и других событиях, создающих предпосылки для несанкционированного доступа к ИКТ.

10.1.7. Представлять письменные объяснения о допущенных нарушениях установленного порядка работы, учета и хранения материальных носителей ИКТ, а также о фактах разглашения ИКТ.

10.1.8. Оказывать помощь и содействие при проведении внутренних служебных расследований по фактам нарушения режима коммерческой тайны, попыток его нарушения или подготовки к нарушению.

10.1.9. Возместить причиненный работодателю ущерб, если работник виновен в разглашении информации, составляющей коммерческую тайну, ставшую ему известной в связи с исполнением им трудовых обязанностей.

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

10.2.1. Передать работодателю (определенному им лицу) все имеющиеся у него документы и носители ИКТ, полученные и/или созданные им в рамках выполнения трудовых обязанностей и/или заданий работодателя.

10.2.2. Не разглашать ИКТ, ставшую известной в период срока действия трудового (гражданско-правового) договора, в течение всего срока действия режима коммерческой тайны в Обществе, в том числе после прекращения действия трудового (гражданско-правового) договора.

10.3. Работнику, имеющему доступ к ИКТ, запрещается:

10.3.1. Распространять, передавать и/или предоставлять сведения, содержащие ИКТ, как на материальных носителях, так и в электронном виде, без нанесения грифа «Коммерческая тайна», полного наименования и местонахождения Общества.

10.3.2. Передавать материальные носители ИКТ без документального подтверждения факта передачи (реестра, акта, подписи получившего на 2-м экземпляре).

10.3.3. Передавать материальные носители ИКТ лицам, не имеющим допуска к работе с ИКТ, или знакомить их с такими сведениями в любой форме.

10.3.4. Передавать ИКТ в электронном виде по незащищенным техническим каналам связи без использования средств защиты информации, принятых Обществом в эксплуатацию в установленном порядке или определенных к использованию Департаментом безопасности.

10.3.5. Использовать ИКТ при осуществлении научной и педагогической деятельности, в открытой переписке, публикациях в СМИ, различного рода публичных выступлениях, а также в личных интересах.

10.3.6. Снимать копии с документов и других носителей ИКТ, а равно использовать различные технические средства (фотоаппараты, видео- и звукозаписывающую аппаратуру) для записи ИКТ без разрешения непосредственного руководителя структурного подразделения.

10.3.7. Сохранять документы и иную ИКТ в электронном виде на носители, не учтенные предварительно в установленном порядке в качестве материальных носителей ИКТ, копировать эту информацию на неучтенные носители.

10.3.8. Оставлять без присмотра документы и материальные носители ИКТ, в том числе в местах для печати и ксерокопирования, а также средства автоматизации (ПК, ноутбуки, смартфоны и т.п.), посредством которых ведется обработка ИКТ в электронном виде, без блокировки доступа к ним.

10.3.9. Выносить материальные носители ИКТ из зданий Общества, а также выполнять какие-либо работы, связанные с ИКТ, вне служебных помещений без разрешения на то непосредственного руководителя структурного подразделения.

10.3.10. Использовать ИКТ, ставшую ему известной в ходе трудовой деятельности в Обществе, для занятия любыми видами деятельности, не связанными с выполнением трудовых обязанностей.

10.4. Обязанности работника Общества по соблюдению требований режима коммерческой тайны и его ответственность за разглашение ИКТ отражаются в заключаемом с работником трудовом договоре или дополнительном соглашении к трудовому договору, а также в положениях о структурных подразделениях и должностных инструкциях работников.

XI. Регулирование отношений, связанных с коммерческой тайной, с контрагентами

11.1. Отношения Общества с контрагентами, которым Обществом передает ИКТ или от которых Общество получает ИКТ, регулируются Соглашениями о конфиденциальности (пункт 11.4 настоящего Положения) между Обществом и контрагентами.

11.2. Общество вправе и обязано требовать охрану конфиденциальности ИКТ Общества и/или его контрагентов от организаций и лиц, получивших доступ к этой информации в результате действий, осуществленных случайно или по ошибке.

11.3. Передача контрагентам ИКТ допускается только при наличии Соглашения о конфиденциальности или договора, заключенного между Обществом и контрагентом, существенным условием которого является охрана конфиденциальности передаваемой информации. В этих целях в договоре предусматривается специальный раздел о конфиденциальности.

11.4. Правила подготовки и содержания договоров определены в СТО.ОСК.КСМК 00-024 «Порядок ведения договорной работы». Типовая форма Соглашения о конфиденциальности утверждена приказом АО «ОСК» от 15 февраля 2022 г. № 40 «Об утверждении типовых форм договоров».

11.5. Раздел о конфиденциальности гражданско-правового договора (или, если применимо, иной раздел гражданско-правового договора) или договор (соглашение) о конфиденциальности должны содержать следующие обязательные условия:

11.5.1. Определение предмета договора и ИКТ.

11.5.2. Порядок, условия передачи, получения и использования ИКТ.

11.5.3. Ответственность сторон договора.

11.5.4. Прочие условия: порядок определения момента вступления договора в силу и срок его действия, применимое право, процедура разрешения споров сторон, ретрансляция условий соглашения о конфиденциальности информации в договоры с третьим лицами, привлекаемыми контрагентом в целях исполнения обязательств перед Обществом.

11.6. Договоры между Обществом и контрагентами о передаче ИКТ могут предусматривать или не предусматривать возможность использования передаваемой ИКТ в целях извлечения прибыли контрагентом, что закрепляется непосредственно в тексте договора.

11.7. В случаях, когда требуется передача контрагенту ИКТ, до начала переговоров между Обществом и контрагентом заключается соглашение о конфиденциальности, а контрагенту передается минимально возможная ИКТ, без предоставления которой оказание услуг Обществу исполнителем, заключение договоров и иные действия были бы невозможны.

11.8. При заключении Соглашений о конфиденциальности с иностранными компаниями-контрагентами в целях защиты интересов Общества необходимо включать в Соглашения о конфиденциальности положения о распространении на предмет договора права Российской Федерации, рассмотрении возможных споров в арбитражных или третейских судах на территории Российской Федерации.

11.9. Текст Соглашения о конфиденциальности должен составляться на русском языке или двух языках – русском и английском, при этом в тексте Соглашения о конфиденциальности в обязательном порядке указывается, что, в случае возникновения противоречия между русской и английской версией Соглашения, версия на русском языке будет иметь преимущественную силу. В исключительных случаях возможно составление Соглашения о конфиденциальности на английском языке, при этом подразделение, ответственное за заключение Соглашения о конфиденциальности, по требованию заинтересованных подразделений, обязано обеспечить оформление официально заверенного перевода договора и всех изменений к нему на русский язык в целях одобрения договора и/или изменений к нему заинтересованными подразделениями.

11.10. Ответственность за принятие решения о составе, объеме, порядке передачи и использования ИКТ, предоставляемой контрагенту, возлагается на исполнителя.

11.11. Передача ИКТ контрагентам в соответствии с заключенными Соглашениями о конфиденциальности производится только на материальных

носителях, на которые нанесен гриф «Коммерческая тайна» с регистрацией факта передачи (отправки документов) в соответствующих формах учета.

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

11.13. Материальные носители (документы), содержащие ИКТ 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.

11.14. Направление контрагентам ИКТ в электронном виде с использованием средств связи общего пользования и сети Интернет (по электронной почте) допускается только при условии использования средств защиты информации, принятых Обществом и контрагентом в эксплуатацию в установленном порядке или определенных к использованию Департаментом безопасности, а также наличия соглашения между Обществом и контрагентом о ведении электронного документооборота, в котором регулируются вопросы охраны конфиденциальности, подтверждения подлинности и авторства документов.

11.15. Во всех остальных случаях использование незащищенных каналов связи для передачи ИКТ запрещается.

ХII. Проведение переговоров с контрагентами по вопросам, требующим ознакомления участников с ИКТ

12.1. Переговоры, рабочие встречи, консультации, совещания с контрагентами по вопросам, требующим ознакомления участников переговоров с ИКТ (далее - переговоры), проводятся только после заключения Обществом со всеми участниками переговоров (контрагентами и/или физическими лицами) гражданско-правовых договоров, регулирующих охрану конфиденциальности ИКТ, в которых определен порядок проведения совещаний, предусматривающих раскрытие ИКТ в устной форме.

12.2. Результаты переговоров, на которых рассматривалась ИКТ, оформляются в виде протоколов, в которых указывается:

12.2.1. Полный состав участников от каждой из сторон переговоров с указанием фамилий, имен, отчеств (при наличии) и должностей, занимаемых участниками переговоров, наименований организаций, которые они представляют.

12.2.2. Краткое содержание обсуждаемой ИКТ с указанием номеров пунктов Перечня ИКТ, относящих данную информацию к коммерческой тайне.

12.2.3. Факт ознакомления участников переговоров с мерами ответственности за разглашение (неправомерное использование) ИКТ.

12.3. На протокол наносится гриф «Коммерческая тайна».

12.4. Протокол подписывается ответственным за проведение совещания.

ХIII. Предоставление ИКТ органам государственной власти

13.1. Предоставление ИКТ 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 затребования ИКТ, срок предоставления этой информации, если иное не установлено законодательством Российской Федерации.

13.2. Общество обязано предоставлять ИКТ по запросам судов, органов прокуратуры, органов предварительного следствия и дознания по делам, находящимся в их производстве, субъектам оперативно-розыскной деятельности в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.

13.3. Предоставление ИКТ органам власти без запроса от них производится в случаях, когда такое предоставление обязательно и необходимо для совершения действий в интересах Общества (оформление паспорта сделки, получение лицензий, государственная регистрация результатов интеллектуальной деятельности, обращение в суд и т.п.).

13.4. Запросы органов власти на предоставление ИКТ принимаются только в письменном виде. Устные запросы на предоставление ИКТ, в том числе полученные по телефону, к рассмотрению не принимаются, о чем необходимо сообщить лицу, направляющему запрос, и указать на наличие такой нормы в законодательстве Российской Федерации о коммерческой тайне.

13.5. 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.

13.6. Запросы органов власти по электронной почте принимаются к рассмотрению только в том случае, если доменный адрес почтовой системы принадлежит соответствующему органу власти. В случаях, когда адрес электронной почты отправителя запроса получен в общедоступной почтовой системе (mail.ru,

rambler.ru, gmail.com, yandex.ru и им подобных), запрос к рассмотрению не принимается, о чем уведомляется отправитель запроса на указанный им электронный адрес. В случае, если работник, готовящий ответ на запрос органа власти, не может определить принадлежность почтового ящика инициатора запроса, он обязан обратиться в ДЦТиИТ и получить там письменное заключение о принадлежности почтового ящика отправителя.

13.7. Проведение проверки указанных выше сведений возлагается на работника Общества, которому поручена подготовка ответа по запросу органа власти. О результатах проверки составляется служебная записка, которая подписывается лицом, проводившим проверку, и прикладывается к проекту ответа на полученный запрос.

13.8. 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 Российской Федерации. Предоставление ИКТ органам власти в электронном виде с использованием средств связи общего пользования (в том числе по факсу) и сети Интернет (по электронной почте) запрещается. Все ответы на запросы, содержащие ИКТ, 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.

13.9. Исключения допускаются только в случае наличия с органами власти каналов связи, закрытых с использованием сертифицированных ФСБ России средств криптографической защиты информации (например, предназначенных для сдачи налоговой, пенсионной и иной отчетности, сервисами электронной подачи (регистрации) результатов интеллектуальной деятельности), 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.

13.10. Если в формах электронной отчетности органов власти отсутствуют поля (графы), позволяющие указать, что предоставляемые сведения относятся к ИКТ, об этом сообщается в орган власти любым документируемым способом (почтой, факсимильным сообщением, электронной почтой), имеющим систему подтверждения доставки корреспонденции, или письмом, доставляемым нарочным с получением расписки принявшего такое письмо лица о его получении.

13.11. В случаях, когда между получением информации в электронном виде и письменным уведомлением Обществом об отнесении ее к ИКТ возможен

временной интервал более суток, о наличии ИКТ в электронном отчете в орган власти сообщается по телефону работником, отправившим соответствующий электронный отчет, с обязательным направлением сообщения в письменной форме.

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

13.13. Ответы на запросы органов власти о предоставлении ИКТ подписываются генеральным директором Общества или лицом, его замещающим, его заместителями (в пределах их полномочий по распоряжению конкретными группами сведений), а также работниками на основании доверенности, которые несут персональную ответственность за соответствие передачи информации интересам Общества и оценку законности ее истребования.

13.14. Решение об отказе органу власти в предоставлении запрашиваемой ИКТ принимается только генеральным директором Общества или лицом, его замещающим, а также работниками на основании доверенности, с предоставлением мотивированного заключения, подготовленного соответствующим структурным подразделением Общества и согласованным с директором Департамента правового обеспечения (лицом, его замещающим).

XIV. Особенности обращения с документами, содержащими информацию, составляющую коммерческую тайну

14.1. Организация работы с документами, содержащими ИКТ, должна обеспечить выполнение следующих основных требований:

14.1.1. Возможность ознакомления с документами, содержащими ИКТ, только работников, имеющих соответствующие права доступа и принявших на себя обязательства по неразглашению коммерческой тайны.

14.1.2. Фиксирование всех фактов передачи документов, содержащих ИКТ, между работниками Общества и предоставление (передачу) их контрагентам и органам власти.

14.1.3. Обеспечение персональной ответственности за сохранность документов, содержащих ИКТ, возможность установить место нахождения документа и лицо, осуществляющее его хранение, в любой промежуток времени.

14.1.4. Возможность изготовления копий документов, содержащих ИКТ, только лицами, имеющими допуск к ИКТ или по поручению соответствующего руководителя, являющегося лицом, имеющим допуск к ИКТ.

14.1.5. Хранение документов только в местах, исключаящих несанкционированный доступ к ним лиц, не имеющих на то прав.

14.2. Организация процессов документооборота (в том числе электронного) и делопроизводства в части ИКТ осуществляется структурными подразделениями в установленном в Обществе порядке согласно Инструкции по делопроизводству в АО «ОСК».

14.3. Вопросы регламентации и реализации мер по организации в Обществе процесса защищенного электронного документооборота конфиденциальной информации ограниченного доступа, в том числе ИКТ, находятся в зоне ответственности Департамента безопасности.

XV. Уничтожение материальных носителей ИКТ

15.1. Уничтожение материальных носителей ИКТ (документов, изданий и машинных носителей) осуществляется постоянно действующей экспертной комиссией АО «ОСК» по проведению экспертизы ценности документов, в которую включаются представители Департамента безопасности и подразделений, в ведении (компетенции) которых находятся сведения с ИКТ, содержащиеся на планируемых к уничтожению носителях.

15.2. Комиссия отбирает для уничтожения носители, содержащие сведения, утратившие актуальность, дальнейшее хранение которых, в том числе архивное, не требуется, а также носители, пришедшие в негодность, дальнейшее использование которых невозможно. Отобранные носители вносятся в составленный комиссией акт об уничтожении (форма акта приведена в приложении № 3 к Положению).

15.3. Подготовленный акт об уничтожении носителей ИКТ подписывается членами комиссии и утверждается генеральным директором Общества. После утверждения акта документы уничтожаются, факт уничтожения документов заверяется членами комиссии.

15.4. Уничтожение материальных носителей ИКТ должно обеспечивать их полное физическое уничтожение: разрезание, сжигание, механическое уничтожение, сдача предприятию по утилизации вторичного сырья, либо гарантированное удаление ИКТ способами, не позволяющими восстановить данные (затирание данных на накопителях на жестких магнитных дисках (НЖМД), SSD, flash в несколько проходов с применением алгоритмов DOD 5220.22, NSA и т.п.).

15.5. Уничтожение носителей информации на бумажной основе производится с применением бумагорезательных машин (шредеров), путем сжигания их в специально оборудованных печах или такие носители передаются для последующего уничтожения предприятию по утилизации вторичного сырья.

15.6. В случае уничтожения материальных носителей специализированным предприятием по утилизации вторичного сырья в договоре с таким предприятием должна предусматриваться обязанность предприятия-утилизатора обеспечить конфиденциальность данных, находящихся на уничтожаемых (утилизируемых) носителях, и кроме того, уничтожение должно осуществляться только под личным наблюдением уполномоченного работника Общества.

15.7. Категорически запрещается передавать средства вычислительной техники без извлечения из них учетных жестких дисков, предназначенных для хранения ИКТ, на утилизацию, для продажи, использования другими организациями, в рамках благотворительной помощи и т.п. без стирания данных с использованием программ (устройств) гарантированного стирания (уничтожения) данных. В случае невозможности стирания данных соответствующими средствами жесткие диски изымаются и уничтожаются.

15.8. Акты об уничтожении составляются в двух экземплярах.

15.9. Первые экземпляры актов об уничтожении хранятся в Департаменте управления делами, ведущем учет материальных носителей ИКТ, для простановки соответствующих отметок в учетных формах.

15.10. Вторые экземпляры актов об уничтожении хранятся в структурных подразделениях, в ведении которых находились документы, содержавшие ИКТ.

15.11. Неутвержденные проекты документов, содержащие ИКТ, черновики, перепечатываемые и заменяемые листы таких документов подлежат обязательному уничтожению в бумагорезательных машинах (шредерах). Персональная ответственность за их уничтожение возлагается на исполнителя документа или лицо, перепечатавшее (заменяющее) отдельные листы документа. Выбрасывать проекты документов, черновики, перепечатанные и/или замененные листы в корзины для бумаг, урны или иным способом допускать их бесконтрольную утилизацию категорически запрещено.

XVI. Ежегодная проверка наличия материальных носителей информации, составляющей коммерческую тайну

16.1. Ежегодно, в период с 15 января по 15 февраля, приказом Общества назначается комиссия по проверке наличия материальных носителей ИКТ. В состав комиссии включаются представители Департамента безопасности, ДЦТиИТ, ДУП, Департамента управления делами и подразделений, в которых ведется работа с материальными носителями ИКТ. По результатам проверки членами комиссии составляется акт (приложение № 4), который утверждается генеральным директором Общества. В указанном акте отражается наличие материальных

носителей ИКТ, причины их отсутствия в случае выявления таких фактов, обнаруженные нарушения режима коммерческой тайны.

16.2. На эту же комиссию возлагается проверка наличия носителей информации ограниченного доступа, имеющих иные ограничительные грифы (пометки) и т.п., на которых могут содержаться персональные данные различных категорий субъектов (абонентов, клиентов, работников, контрагентов), информация, полученная от контрагентов и т.п.

XVII. Ответственность за нарушение порядка обращения с информацией, составляющей коммерческую тайну

17.1. Невыполнение работником Общества требований настоящего Положения и причинение Обществу, его контрагентам убытков вследствие разглашения ИКТ или ее неправомерного использования влечет за собой дисциплинарную, материальную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

17.2. Разглашение ИКТ является инцидентом информационной безопасности и влечет за собой последствия, предусмотренные законодательством Российской Федерации, а также договорными обязательствами между Обществом и его работником.

17.3. В целях предотвращения разглашения ИКТ и/или создания предпосылок к этому Общество оставляет за собой право, но не принимает каких-либо обязательств контролировать любыми доступными законными способами надлежащее использование работниками технических средств хранения, обработки и передачи информации, соблюдение им установленных режимных мер по охране конфиденциальности ИКТ.

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

17.5. По каждому факту разглашения ИКТ, создания к этому предпосылок или нарушению работником установленных режимных мер по охране конфиденциальности ИКТ 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 осуществляющие контроль, предусмотренный локальными нормативными актами Общества), к виновным принимаются меры воздействия, а в систему охраны конфиденциальности вносятся изменения, препятствующие возникновению подобных инцидентов в дальнейшем. Порядок проведения разбирательства определяется Инструкцией по управлению инцидентами информационной безопасности в АО «ОСК» (ОСК.СМК 00-168).

17.6. Ответственность за разглашение ИКТ несет персонально работник Общества, имеющий доступ к этим сведениям и допустивший их утечку (разглашение).

17.7. Руководство Общества принимает решение о взыскании с виновных лиц убытков, нанесенных нарушением права Общества на ИКТ, в порядке, предусмотренном законодательством Российской Федерации.

17.8. При наличии в действиях работника Общества, разгласившего ИКТ, признаков административного правонарушения или уголовного преступления, руководство Общества по заявлению уполномоченных должностных лиц имеет право обратиться в соответствующие государственные органы для привлечения его к ответственности в соответствии с законодательством Российской Федерации.

17.9. При причинении работником убытков Обществу вследствие разглашения ИКТ, ставшей ему известной в связи с исполнением им трудовых обязанностей, работник обязан возместить причиненный вред в соответствии с положениями законодательства Российской Федерации.

17.10. При отказе работником возместить причиненный Обществу вред руководство Общества имеет право обратиться в суд за защитой своих интересов.

17.11. При выявлении нарушения требований режима коммерческой тайны к работнику Общества, допустившему нарушение, могут быть применены меры дисциплинарного взыскания. Трудовой договор с работником может быть расторгнут по инициативе Общества в случае разглашения им ИКТ, ставшей известной работнику в связи с исполнением им трудовых обязанностей, на основании подпункта «в» пункта 6 статьи 81 Трудового кодекса Российской Федерации.

XVIII. Заключительные положения

18.1. Настоящее Положение вступает в силу с момента его утверждения.

18.2. Учет ознакомлений работников АО «ОСК» с настоящим Положением ведется ДУП при оформлении и подписании с работником АО «ОСК» обязательства о сохранении коммерческой тайны и иной информации ограниченного доступа (трудового договора).

18.3. Доведение требований Положения до сведения всех работников АО «ОСК» осуществляется путем размещения документа в корпоративной сети на информационном портале, а также посредством СЭД в установленном порядке.

18.4. Порядок подготовки и работы с документами, содержащими ИКТ, осуществляется в порядке, определенном в приложении № 5.

18.5. Контроль за соблюдением требований Положения осуществляется Департаментом безопасности АО «ОСК» на плановой и (или) внеплановой основе.

Приложение № 1
к Положению
о коммерческой тайне АО «ОСК»

Акционерное общество
«ОБЪЕДИНЕННАЯ СУДОСТРОИТЕЛЬНАЯ КОРПОРАЦИЯ»
ОБЯЗАТЕЛЬСТВО

О СОХРАНЕНИИ КОММЕРЧЕСКОЙ ТАЙНЫ И ИНОЙ
ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

1. Я, _____,
(Ф.И.О)

как лицо, состоящее в трудовых или гражданско-правовых отношениях с акционерным обществом «Объединенная судостроительная корпорация» (далее – АО «ОСК», Общество), предупрежден и осознаю, что в процессе работы получу доступ к информации АО «ОСК», составляющей коммерческую тайну, служебную тайну, персональные данные и иную информацию, в отношении которой законодательно установлены требования о соблюдении режима конфиденциальности (далее – информация ограниченного доступа).

2. Я ознакомлен с требованиями действующего законодательства Российской Федерации, локальными нормативными актами, приказами (распоряжениями) АО «ОСК» по вопросам защиты информации ограниченного доступа и обязуюсь в период трудовых или иных гражданско-правовых отношений с АО «ОСК» (ее правопреемником) и в течение трех лет после их окончания, если более длительный срок не установлен локальными нормативными актами или иными документами АО «ОСК»:

2.1. Не использовать для личных целей и собственной выгоды, в том числе для занятия любыми видами деятельности, не разглашать (устно или письменно) сведения, составляющие коммерческую тайну АО «ОСК», и иную информацию ограниченного доступа, ставшую известной в связи с выполнением трудовых обязанностей.

2.2. Не подписывать и не подтверждать в устной форме какие-либо гарантии и/или обязательства от имени АО «ОСК» без письменных полномочий, не передавать и не распространять иным способом информацию об Обществе или сведения, полученные при исполнении трудовых обязанностей, которые могут

нанести репутационный/деловой ущерб, не делать публичных заявлений от имени АО «ОСК» без соответствующих полномочий, предоставленных Обществом.

2.3. Соблюдать режим конфиденциальности информации ограниченного доступа, установленный в АО «ОСК», в том числе соблюдать порядок обработки и защиты информации ограниченного доступа.

2.4. Использовать предоставленные АО «ОСК» технические средства хранения, обработки и передачи информации ограниченного доступа, документы и материалы, содержащие информацию ограниченного доступа, и средства доступа к данной информации исключительно для выполнения трудовых обязанностей.

2.5. Немедленно сообщать непосредственному руководителю и представителю Департамента безопасности АО «ОСК» о попытке третьих лиц получить информацию ограниченного доступа и о любой потенциальной угрозе, которая может привести к разглашению информации ограниченного доступа, в том числе в случаях утраты средств хранения, обработки и передачи информации ограниченного доступа, документов, содержащих информацию ограниченного доступа, и средств доступа к данной информации.

2.6. Сохранять ставшую мне известной в связи с трудовой деятельностью или гражданско-правовыми отношениями служебную тайну министерств и ведомств Российской Федерации, а также коммерческую тайну тех предприятий, с которыми у АО «ОСК» имеются деловые (партнерские) отношения.

2.7. Не использовать знания коммерческой тайны АО «ОСК» и иной информации ограниченного доступа для занятия любой деятельностью, которая в качестве конкурентного действия может нанести ущерб Обществу.

2.8. В случае моего увольнения не позднее последнего рабочего дня вернуть АО «ОСК» технические средства хранения, обработки и передачи информации ограниченного доступа, документы, содержащие информацию ограниченного доступа, и средства доступа к данной информации, которые находились в моем распоряжении в связи с выполнением трудовых обязанностей.

2.9. Об утрате или недостатке носителей коммерческой тайны АО «ОСК» и иной конфиденциальной информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), и о других фактах, которые могут привести к разглашению или утечке информации ограниченного доступа, немедленно сообщить в Департамент безопасности АО «ОСК».

3. Я предупрежден о том, что в случае невыполнения мною любого из вышеперечисленных пунктов настоящего обязательства и нарушениях этих положений в отношении меня в соответствии с действующим законодательством Российской Федерации могут быть применены установленные меры дисциплинарной, административной, гражданско-правовой, уголовной

ответственности, включая обязанность по возмещению причиненных АО «ОСК» убытков.

4. Общество вправе контролировать надлежащее использование предоставленных мне АО «ОСК» документов, содержащих информацию ограниченного доступа, технических средств хранения, обработки и передачи информации, соблюдение мною мер по соблюдению конфиденциальности информации ограниченного доступа.

5. Подписанием настоящего обязательства даю свое согласие на осуществление АО «ОСК» контроля (мониторинга) за надлежащим использованием мною предоставленных Обществом документов и материалов, содержащих информацию ограниченного доступа, технических средств хранения, обработки и передачи информации, соблюдением мною мер по охране конфиденциальности информации ограниченного доступа и обязуюсь не препятствовать Обществу осуществлять данный контроль.

6. Настоящее обязательство может быть дополнено или изменено только по письменному соглашению Работодателя и Работника.

8. Настоящее обязательство составлено в двух экземплярах, каждый из которых имеет одинаковую юридическую силу.

9. Невыполнение условий настоящего обязательства влечет дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

10. Руководство АО «ОСК» подтверждает, что данные Вами обязательства о сохранении коммерческой тайны и иной информации ограниченного доступа не ограничивают Ваших прав выезда за рубеж.

(подпись)

(расшифровка)

(дата)

Директор Департамента
управления персоналом

/Э.В.Бобрицкий

Один экземпляр настоящего обязательства получил

(подпись)

(расшифровка)

(дата)

Приложение № 3
к Положению
о коммерческой тайне АО «ОСК»

Шаблон акта уничтожения носителей информации, составляющей коммерческую тайну АО «ОСК», не подлежащих дальнейшему хранению

Разрешаю уничтожить

(должность лица, назначившего комиссию)

(подпись, инициалы, фамилия)

« _____ » _____ 20__ г.

Комиссия в составе

председатель

(должность, инициалы, фамилия)

члены

(должность, инициалы, фамилия)

(должность, инициалы, фамилия)

провела отбор материальных носителей информации, составляющей коммерческую тайну АО «ОСК», и установила, что в соответствии с требованиями локальных нормативных актов АО «ОСК» не подлежат дальнейшему хранению и использованию следующие носители информации, составляющей коммерческую тайну:

№ п/п	Регистрационный номер носителя	Наименование документа (носителя)	Количество экземпляров/ номера экземпляров	Общее количество листов в каждом экземпляре (если применимо)	Примечание
1	2	3	4	5	7

После утверждения акта перечисленные носители сверены с записями в акте и уничтожены путем

(разрезания в бумагорезательной машине, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

(подписи членов комиссии)

(инициалы и фамилии членов комиссии)

Приложение № 4
к Положению
о коммерческой тайне АО «ОСК»

Шаблон акта проверки наличия материальных носителей информации, составляющей коммерческую тайну АО «ОСК», и иной информации ограниченного доступа

УТВЕРЖДАЮ

(должность лица, назначившего комиссию)

(подпись, инициалы, фамилия)

« _____ » _____ 20__ г.

Комиссия в составе

председатель

(должность, инициалы, фамилия)

члены

(должность, инициалы, фамилия)

(должность, инициалы, фамилия)

осуществила проверку материальных носителей информации, составляющей коммерческую тайну АО «ОСК», и иной информации ограниченного доступа, зарегистрированных в формах первичного учета, и установила наличие следующих носителей:

№ пп	Регистрационный номер, дата регистрации носителя (документа, дела)	Наименование (заголовок) носителя (документа, дела)	Подпись члена комиссии	ФИО члена комиссии и дата проверки
1	2	3	4	5

В период работы комиссии _____

_____.

(указываются выявленные факты отсутствия материальных носителей, вскрытые факты нарушения режима коммерческой тайны, если таковые имеются, предлагаемые меры по устранению нарушений режима коммерческой тайны)

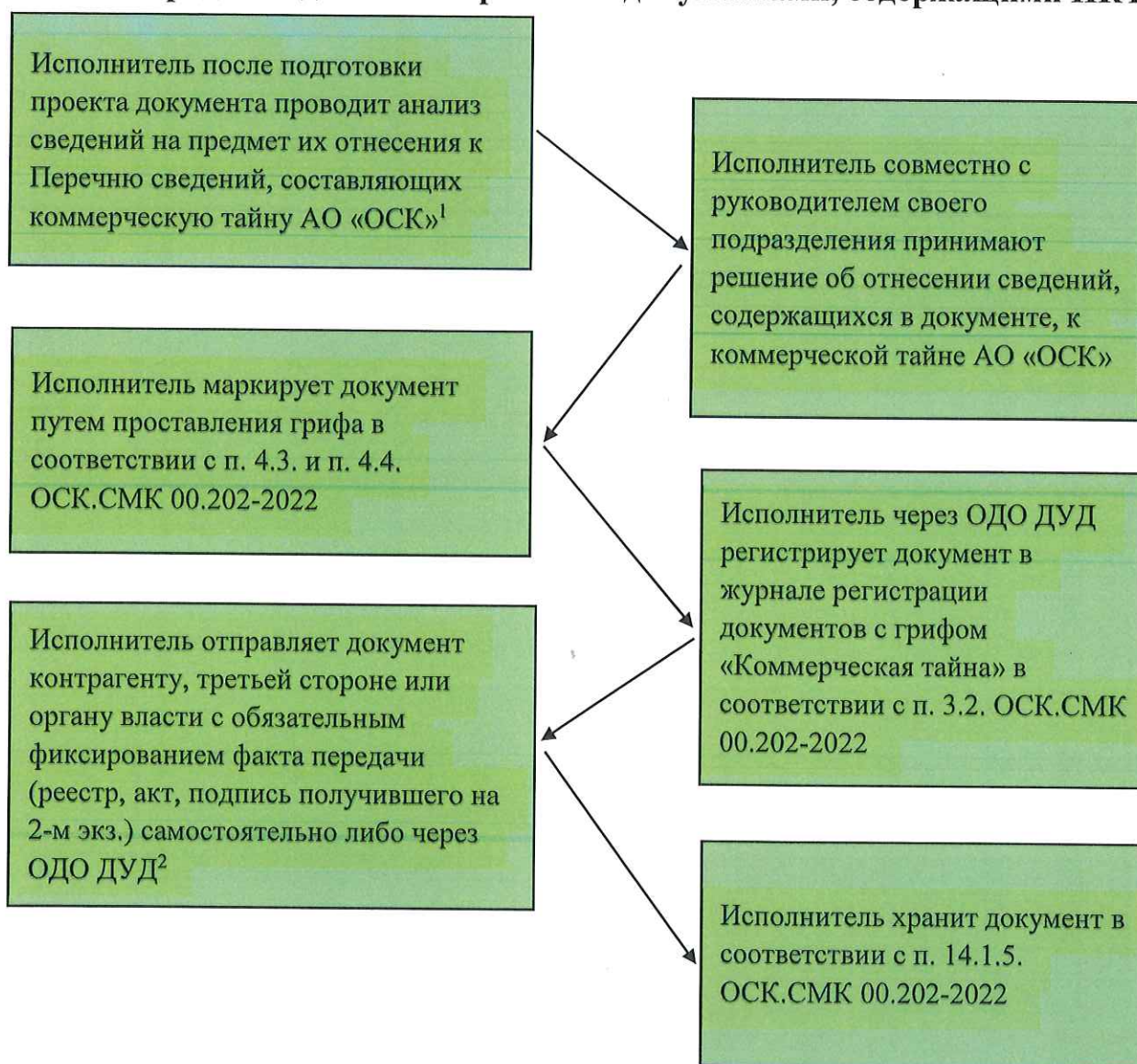
(подписи членов комиссии)

(инициалы и фамилии членов комиссии)

« _____ » _____ 202__ г.

Приложение № 5
к Положению
о коммерческой тайне АО «ОСК»

Порядок подготовки и работы с документами, содержащими ИКТ



1. Если информация относится к категории «Служебная тайна в области обороны», то необходимо руководствоваться постановлением Правительства Российской Федерации от 26 ноября 2021 г. № 2052 и маркировать документ грифом «Для служебного пользования».

2. Отправка документов осуществляется только при наличии подписанного Соглашения о конфиденциальности. Отправка ИКТ в органы власти осуществляется только на основании письменного мотивированного запроса от органов власти.

Передача документов допускается только по защищенным каналам связи (шифротелеграммой, посредством «Континента», ПО «Крипто АРМ» или VipNet), либо нарочным, курьером, фельдъегерской службой в опечатанном виде, не допускающем ознакомления с содержимым.