Утверждено:
Приказом № _____ от «___» _____ 201_ года
Генеральный директор
ОАО «ФИРМА»

Ф.И.О.

ПОЛОЖЕНИЕ
о защите информации, содержащей сведения конфиденциального характера в ОАО «ФИРМА»

Город
201_ г.

1. Общие положения.
   1.1. Положение о защите информации, содержащей сведения конфиденциального характера (далее – Положение) разработано в соответствии с Конституцией РФ, Гражданским кодексом РФ, Трудовым кодексом РФ, другими нормативно-правовыми актами Российской Федерации, регулирующими отношения в области информации (Приложение №1), Уставом и Концепцией безопасности информации ОАО «ФИРМА» (далее – Общество).
   1.2. Положение вводит категорирование информации, в зависимости от степени ее конфиденциальности и определяет режим конфиденциальности в ОАО «ФИРМА» (далее - Общество) по отношению к информации[1], содержащей сведения конфиденциального характера [12], хранимой и обрабатываемой в Обществе, и регламентирует меры по ее защите, с целью предотвращения нанесения возможного ущерба интересам и деловой репутации Общества, вызванного умышленными или неосторожными действиями работников Общества, других юридических и физических лиц вследствие разглашения (передачи, утраты) или незаконного присвоения такой информации.

   При реорганизации Общества (в форме слияния, присоединения, разделения, выделения или преобразования) право на установление, изменение или отмену режима конфиденциальности переходит к его правопреемнику.
   1.3. Положение является руководящим документом, единым для всего Общества, обязательным для выполнения всеми работниками Общества. Положением определяются обязанности работников и должностных лиц Общества по обеспечению режима конфиденциальности, и вводится ответственность за нарушение этого режима.
   1.4. Сохранение сведений конфиденциального характера является неотъемлемой частью деятельности Общества.
   1.5. Защита сведений конфиденциального характера не может быть использована для сокрытия фактов бесхозяйственности, недобросовестной конкуренции и других негативных явлений в деятельности Общества.
   1.6. Настоящее Положение вступает в силу с момента его утверждения Приказом Генерального директора Общества и действует без ограничения срока, до замены его новым Положением.
2. Термины и определения.
   2.1. Информация: сведения (сообщения, данные) независимо от формы их представления [2].
   2.2. Документ (документированная информация): зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель [2].
   2.3. Носитель информации: материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин [9].
   2.4. Обладатель информации: лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [2].
   2.5. Конфиденциальность информации: обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [2].
   2.6. Режим конфиденциальности: организационные, технические и иные меры по защите конфиденциальной информации, принимаемые ее обладателем на основании закона

[1] Предметом рассмотрения данного Положения является документированная информация (см. п. 2.2).

или договора.

2.7. Доступ к информации: возможность получения информации и ее использования [2].

2.8. Информация, составляющая коммерческую тайну (секрет производства): 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 коммерческой тайны [3].

2.9. Персональные данные: любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация [4].

2.10. Обезличивание персональных данных: действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных [4].

2.11. Общедоступные персональные данные: персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности [4].

2.12. Политика безопасности (информации в организации): совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности [9];

2.13. Руководители структурных подразделений: директора, начальники служб, отделов, их заместители, возглавляющие подразделения, напрямую подчиненные Генеральному директору Общества.

3. Категорирование информации по степени конфиденциальности.

Данным Положением в Обществе вводятся следующие категории информации:

- информация, содержащая сведения, составляющие охраняемую законом тайну (государственную, служебную, профессиональную, коммерческую или иную тайну);
- внутренняя информация ограниченного распространения (обращения);
- общедоступная информация.

3.1. Информация, содержащая сведения, составляющие охраняемую законом тайну (далее – ИОЗТ).

К данной категории относится:

- информация, содержащая сведения конфиденциального характера [12], доступ к которой должен быть ограничен и приняты меры по ее защите, в соответствии с требованиями Федеральных законов [2, 3, 4]:
    - информация, составляющая коммерческую тайну Общества;
    - информация, составляющая государственную тайну;
    - персональные данные работников Общества.

3.1.1. Информация, составляющая коммерческую тайну Общества.

Право на отнесение информации к информации, составляющей коммерческую тайну и на определение перечня и состава такой информации, согласно [3], принадлежит Обществу, за исключением информации, содержащей сведения, перечисленные в статье 5 [3] и [7].

Сведения, составляющие коммерческую тайну, определяются «Перечнем сведений, составляющих коммерческую тайну ОАО «ФИРМА» (далее – Перечень СКТ).

Перечень СКТ, является единым для всего Общества, разрабатывается на основе

предложений руководителей структурных подразделений Общества Дирекцией по режиму и экономической безопасности (далее – ДРиЭБ) и утверждается приказом Генерального директора Общества.

Изменения и дополнения к Перечню рассматриваются ДРиЭБ на основании предложений руководителей структурных подразделений Общества и вносятся в него приказом Генерального директора Общества по представлению ДРиЭБ.

3.1.2. Персональные данные работников Общества.

Информация, содержащая персональные данные всегда относится к категории конфиденциальной информации, за исключением случаев:

- обезличивания персональных данных (см. п. 2.11);
- иных случаях установленных Федеральным законом «О персональных данных» и иными федеральными нормативными актами.

Обработка персональных данных осуществляется в порядке и на условиях предусмотренных действующим законодательством, при условии письменного согласия работника, содержащего перечень персональных данных и цель их обработки. Исключение составляет случай, когда обработка персональных данных осуществляется в целях исполнения трудового или гражданско-правового договора с субъектом персональных данных.

Согласие, подписанное работником, приобщается к его личному делу и хранится в течение всего срока, определенного для хранения личных дел.

3.2. Внутренняя информация ограниченного распространения (обращения) (далее – ВИОР).

К данной категории относится:

3.2.1. Внутренняя информация, которая не содержит сведений конфиденциального характера [12], распространение (обращение) которой в Обществе (вне Общества), может быть ограничено, исходя из интересов Общества или его структурных подразделений, если это не противоречит действующему законодательству РФ.

Перечень такой информации разрабатывается на основе предложений руководителей структурных подразделений Общества ДРиЭБ и утверждается приказом Генерального директора Общества.

3.2.2. Информация, полученная от третьей стороны на основании договора и на условиях сохранения ее конфиденциальности.

Информация, полученная от третьей стороны, может быть отнесена к данной категории при одновременном соблюдении следующих условий:

- требования третьей стороны о соблюдении конфиденциальности передаваемой информации не противоречат действующему законодательству РФ;
- передача и получение информации осуществляется на основании договора;
- этим договором или отдельным соглашением к нему определены обязательства Общества по сохранению конфиденциальности и ответственность за разглашение этой информации.

Порядок изготовления, регистрации, учета, размножения, хранения и уничтожения документов, содержащих ВИОР, соответствует порядку для обычных документов и определяется Инструкцией «по делопроизводству Общества».

Передача (обращение, распространение) документов, содержащих ВИОР внутри Общества (между структурными подразделениями) и третьим лицам должна осуществляться только с разрешения руководителя структурного подразделения и только с сопроводительным письмом, содержащим предупреждение об ограничении распространения (обращения) документа, после обязательной регистрации в журнале исходящих документов.

Дополнительные меры по защите этой категории информации не предусматриваются.

3.3. Общедоступная информация.

К данной категории относится любая другая информация, не отнесенная к первым

двум категориям, а также информация, определяемая Федеральным законодательством (например, [5]) как общедоступная.

3.4. Определение грифа конфиденциальности для материального носителя информации (информационного ресурса).

3.4.1. Гриф конфиденциальности для носителя информации (информационного ресурса) определяется по категории информации зафиксированной на нем. Если носитель (информационный ресурс) содержит информацию разных категорий конфиденциальности, то гриф присваивается по наивысшей из имеющихся категорий. Форма и содержание наносимого грифа конфиденциальности определяются Инструкциями по делопроизводству.

3.4.2. Гриф конфиденциальности определяет и присваивает руководитель структурного подразделения, в чьем ведении находится носитель информации (информационный ресурс), руководствуясь настоящим Положением, а также иными локальными нормативными актами Общества, изданными во исполнение Положения.

3.4.3. Гриф конфиденциальности наносится всегда на носители (документы) с информацией, составляющей коммерческую тайну Общества. На носители (документы), содержащие персональные данные работников гриф конфиденциальности (предупреждение о конфиденциальности) наносится только при их передаче третьим лицам.

4. Организация работы по защите конфиденциальной информации.

4.1.1. Организация работы по защите ИОЗТ (установлению режима конфиденциальности) Общества и контроль над соблюдением режима конфиденциальности и мер по ее защите, возложена на ДРиЭБ. В этой части ДРиЭБ выполняет следующие функции:

- разработка проектов руководящих документов по вопросам обеспечения режима конфиденциальности, определения порядка обращения с ИОЗТ;
- организация взаимодействия с органами государственной власти, правоохранительными и контролирующими органами, подразделениями безопасности и защиты информации других организаций, координация работы структурных подразделений по вопросам обеспечения и соблюдения режима конфиденциальности;
- переработка (внесение изменений и дополнений) Перечня сведений, составляющих коммерческую тайну;
- рассмотрение возможности передачи ИОЗТ Общества, третьим лицам;
- рассмотрение предложений о снятии ограничений на доступ к информации, составляющей коммерческую тайну, а также о возможности опубликования такой информации на общедоступных ресурсах (раскрытия);
- установление требований к техническому оснащению помещений, в которых осуществляется работа с ИОЗТ;
- получение от имени и по поручению должностных лиц Общества электронных цифровых ключей, изготавливаемых уполномоченными центрами сертификации в целях осуществления информационного обмена между Обществом и государственными, налоговыми органами, государственными фондами, финансовыми учреждениями, изготовление от имени и по поручению должностных лиц Общества дубликатов таких ключей;
- организация освидетельствования (приемки) помещений на предмет их пригодности к проведению работ с ИОЗТ;
- подготовка предложений Генеральному директору о приостановке работ с ИОЗТ (блокированию доступа к ИОЗТ) при наличии предпосылок к ее утечке;
- оценку (самостоятельно или с привлечением специалистов и организаций, в том числе на договорной основе) достаточности принимаемых в Обществе мер по обеспечению режима конфиденциальности;

- анализ и оценка рисков, связанных с нарушением режима конфиденциальности;
- проведение занятий и консультаций сотрудников Общества, по порядку и правилам обращения с ИОЗТ;
- рассмотрение вопросов обеспечения и соблюдения режима конфиденциальности.

4.1.2. Для выполнения своих функций ДРиЭБ имеет право:
- выносить на рассмотрение Генерального директора Общества, вопросы, касающиеся обеспечения и соблюдения режима конфиденциальности;
- привлекать, по согласованию с руководителями структурных подразделений, отдельных специалистов для подготовки проектов локальных нормативных документов по защите ИОЗТ;
- с разрешения Генерального директора Общества производить плановые и внезапные проверки на предмет соблюдения режима конфиденциальности в Обществе;
- запрашивать от всех сотрудников Общества точного выполнения нормативных документов по обеспечению режима конфиденциальности. При необходимости представлять руководителю структурного подразделения, либо Генеральному директору Общества предложения по отстранению от работы с ИОЗТ работников Общества, нарушающих установленные требования по соблюдению режима конфиденциальности, и запрещению обработки ИОЗТ техническими средствами, не обеспечивающими ее защиту от несанкционированного доступа.

4.1.3. Работу ДРиЭБ по организации и защите ИОЗТ координирует Генеральный директор Общества.

5. Меры по защите ИОЗТ.

Защита ИОЗТ Общества, обеспечивается комплексным использованием административных, организационных и технических мер защиты, в том числе:
- определением порядка отнесения сведений к сведениям, составляющим коммерческую тайну, определением и утверждением Перечня таких сведений;
- учетом лиц, получивших доступ к ИОЗТ, и (или) лиц, которым такая информация была предоставлена или передана;
- определением порядка регистрации, учета, размножения, хранения, передачи и уничтожения ИОЗТ и носителей такой информации;
- ограничением доступа к ИОЗТ;
- регулированием отношений по использованию ИОЗТ работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- определением обязанностей работников Общества при работе с ИОЗТ;
- установлением ответственности за разглашение ИОЗТ;
- назначением в структурных подразделениях Общества лиц, ответственных за обеспечение режима конфиденциальности, ведения конфиденциального делопроизводства и контроля над соблюдением режима конфиденциальности в этих подразделениях.
- нанесением на материальные носители (документы), содержащие ИОЗТ, грифа конфиденциальности.

5.1. Допуск работников Общества к работе с ИОЗТ.

5.1.1. Руководитель структурного подразделения формирует список работников своего подразделения, которых необходимо допустить к работе с ИОЗТ, и направляет его на согласование Директору по режиму и экономической безопасности. Директор по режиму и экономической безопасности в течение двух рабочих дней определяет возможность допуска этих лиц.

5.1.2. Окончательное решение о допуске к работе с ИОЗТ по каждому работнику принимает руководитель структурного подразделения после подписания этим работником Обязательства (Приложение № 3) о неразглашении охраняемой законом тайны (далее – Обязательство) и ознакомления (под роспись) с Перечнем СКТ (если необходимо), настоящим Положением и Инструкциями (см. п. 5.2.). Обязательство, подписанное

работником, передается руководителем структурного подразделения в Отдел по управлению персоналом Общества, где приобщается к личному делу работника.

5.1.3. Список работников Общества, допущенных к работе с ИОЗТ, утверждается приказом Генерального директора Общества. Список подлежит обязательному пересмотру не реже одного раза в год. В течение этого периода в него могут вноситься изменения и дополнения по инициативе руководителей структурных подразделений Общества и по представлению Директора по режиму и экономический безопасности.

5.2. Конфиденциальное делопроизводство, обработка персональных данных.

Порядок изготовления, регистрации, учета, размножения, передачи и уничтожения документов и съемных машинных носителей, содержащих сведения, составляющие коммерческую тайну Общества, определяется Инструкцией «По делопроизводству документов, содержащих информацию, составляющую коммерческую тайну ОАО «ФИРМА».

Порядок обработки персональных данных определяется Инструкцией «По обработке персональных данных работников в ОАО «ФИРМА» (далее – Инструкции).

5.3. Требования к помещениям, в которых обрабатывается и хранится ИОЗТ.

5.3.1. Помещения должны располагаться в пределах охраняемого периметра зданий, и оборудованы средствами охранной и пожарной сигнализации;

5.3.2. Окна в помещениях должны быть оборудованы защитными жалюзи или пленками, защищающими от визуального контроля. Окна помещений, расположенных на первых и последних этажах зданий должны быть оборудованы защитными металлическими решетками;

5.3.3. Для хранения документов и носителей информации, содержащих ИОЗТ, в помещениях должны быть установлены сейфы или запираемые на замок металлические шкафы.

5.3.4. Помещения, в которых ведется прием посетителей, должны быть оборудованы защитными барьерами, ограничивающими рабочую зону и предотвращающими свободный проход в нее. При отсутствии таких барьеров работа с документами, содержащими ИОЗТ должна прекращаться на время приема посетителей.

5.3.5. Не допускается использование в этих помещениях фото-, теле-, видео-, радио аппаратуры, средств аудиозаписи, телефонов (факсов) с радио удлинителями, периферийных беспроводных компьютерных устройств во время работы с ИОЗТ.

5.4. Обработка и хранение конфиденциальной информации, представленной в электронном виде.

Конфиденциальная информация представленная в электронном виде может содержаться в отдельных электронных документах (файлах) или в составе баз данных.

5.4.1. Обработка и хранение ИОЗТ допускается только на отдельном, выделенном для этих целей сервере (серверах) информационно - вычислительной сети Общества (далее – ИВС) – сервере (серверах) конфиденциальной информации (далее – СКИ).

5.4.2. Обмен данными между СКИ и другими компьютерами (рабочими станциями, серверами) должен быть организован через защищенные соединения, организованные с использованием протоколов IPSec с проверкой подлинности и шифрованием IP-пакетов.

5.4.3. Запрещается копирование файлов с ИОЗТ и хранение их на жестких дисках рабочих станций (компьютеров, ноутбуков), съемных машинных носителях информации, других устройствах, способных накапливать и хранить информацию в электронном виде, за исключением случаев, описанных в Инструкциях.

5.4.4. Резервное копирование ИОЗТ с СКИ должно производиться на отдельные съемные носители информации. Учет и хранение этих носителей обеспечивает Дирекция по информационным технологиям. Требования к учету и хранению носителей информации с резервными копиями аналогичны требованиям к учету и хранению съемных машинных носителей информации, описанным в Инструкции «По делопроизводству документов, содержащих информацию, составляющую коммерческую

тайну ОАО «ФИРМА».

5.4.5. Администрирование СКИ, внесение изменений в программное и аппаратное обеспечение, резервное копирование и восстановление информации должно осуществляться работниками Дирекции по информационным технологиям, из числа допущенных к работе с конфиденциальной информацией.

5.4.6. Рабочие станции (компьютеры, ноутбуки) пользователей ИВС Общества, работающих с ИОЗТ допускается устанавливать в помещениях, отвечающих требованиям, описанным в подразделе 5.3.

5.4.7. Пользователям ИВС Общества (учетным записям пользователей), работающим с ИОЗТ должны быть запрещены доступ к сети Интернет, и средствам электронной почты.

5.5. Ограничение доступа к ИОЗТ.

5.5.1. Доступ к ИОЗТ должен предоставляться только тем лицам, которым эта информация необходима для выполнения возложенных на них обязанностей и только в том объеме (к той ее части), который необходим для выполнения определенных функций.

5.5.2. Правом предоставления, ограничения, прекращения доступа ко всей ИОЗТ, создаваемой, хранимой и обрабатываемой Обществом, включая информацию, полученную от третьих лиц, обладает Генеральный директор Общества.

5.5.3. Правила и порядок предоставления и контроля доступа к информации определяются другими организационно - распорядительными документами Общества.

5.6. Порядок передачи конфиденциальной информации.

5.6.1. ИОЗТ может быть передана третьей стороне по письменному запросу третьей стороны и только с письменного разрешения Генерального директора Общества при условии соблюдения требований действующего законодательства:

- по требованию органов государственной власти и местного самоуправления, государственных надзорных и контролирующих органов, а также акционеров Общества в соответствии с действующим законодательством РФ;
- членам Совета директоров, других органов Общества в соответствии с локальными нормативными актами Общества;
- другим физическим и юридическим лицам на основании гражданско-правовых договоров, заключенных между ними и Обществом, при условии наличия в этих договорах обязательств по соблюдению режима конфиденциальности в отношении данной информации, ответственности за разглашение этой информации или заключения с ними отдельного договора о конфиденциальности (Приложение №2)[2].

5.6.2. Право принятия решения о передаче ИОЗТ (предоставлении доступа к ней) одного структурного подразделения Общества в другое структурное подразделение принадлежит руководителям этих подразделений.

5.6.3. Необходимость (возможность) передачи ИОЗТ Общества для открытого опубликования (раскрытия), ее объем, форму, и время опубликования (раскрытия) определяет Генеральный директор Общества с учетом, заключения ДРиЭБ, Дирекции по правовым и корпоративным вопросам, а также иных структурных подразделений Общества (при необходимости). Под открытым опубликованием (раскрытием) ИОЗТ понимается ее публикация в открытой печати, компьютерных информационных сетях общего пользования, передача по радио и телевидению, оглашение на международных и российских симпозиумах, совещаниях, конференциях, съездах, при публичных выступлениях и защите диссертаций, вывоз за границу или передача ее в любой форме организациям или отдельным лицам, с которыми не заключен договор о конфиденциальности.

5.6.4. Персональные данные работников Общества могут быть переданы третьей стороне или опубликованы на общедоступных источниках только с письменного согласия

---

[2] Действительно в случаях передачи информации, содержащей сведения, составляющие коммерческую тайну Общества.

этих работников на передачу или опубликование своих персональных данных. В случае передачи персональных данных третьим лицам, эти лица должны быть предупреждены о необходимости соблюдать конфиденциальность полученных персональных данных.

5.6.5. Порядок передачи ИОЗТ внутри Общества и третьим лицам на бумажных и съемных машинных носителях информации определяется Инструкциями. Передача ИОЗТ, представленной в электронном виде (документы, файлы, базы данных, архивы) через сети передачи данных должна осуществляться исключительно в зашифрованном виде, при условии, что только обменивающимся сторонам доступны секретные ключи шифрования (пароли).

5.7. Порядок подготовки и проведения совещаний, встреч, переговоров, аудио и видеоконференций, связанных с обсуждением сведений конфиденциального характера.

Проведение совещаний, встреч, переговоров, аудио и видеоконференций, телефонных переговоров связанных с обсуждением сведений конфиденциального характера без принятия специальных мер, изложенных ниже, не допускается:

- совещания, встречи, переговоры, аудио и видеоконференции, связанные с обсуждением сведений конфиденциального характера должны проводиться в специально выделенных для этих целей помещениях (далее – ВП). Перечень таких помещений составляется ДРиЭБ и утверждается Генеральным директором Общества;
- ВП должны периодически обследоваться специальными организациями, имеющими лицензию на проведение такого вида работ. Периодичность проверок определяется ДРиЭБ и утверждается Генеральным директором Общества;
- для защиты от специальных технических средств перехвата и регистрации информации ВП должны быть оборудованы средствами защиты и приняты все меры, в соответствии с рекомендациями обследующей организации, указанными в акте выполненных работ;
- доступ в ВП должен быть ограничен кругом лиц, участвующих (приглашенных) в совещании;
- запрещается проведение аудио- и видеоконференций, связанных с обсуждением сведений конфиденциального характера без принятия специальных мер защиты информации, передаваемой по незащищенным каналам связи;
- запрещается использование фото-, видео-, аудиозаписи, мобильных телефонов, диктофонов и других технических средств регистрации информации, в том числе, встроенных в портативные и карманные компьютеры, мобильные телефоны, без разрешения должностного лица Общества, ответственного за проведение мероприятия;
- должностные лица Общества, ответственные за проведение мероприятий обязаны ознакомить всех участников с требованиями настоящего Положения об ограничениях в использовании технических средств регистрации информации, о необходимости сохранения в тайне сведений конфиденциального характера (при необходимости уточнить какие именно сведения являются охраняемыми), о чем делается отметка в протоколе совещания (встречи, переговоров, аудио и видеоконференции).

5.8. Обязанности работников Общества, допущенных к работе с ИОЗТ.

5.8.1. Работник Общества, допущенный к работе с ИОЗТ, обязан:

- знать и выполнять требования настоящего Положения, других руководящих документов по защите информации, а также знать Перечень сведений, составляющих коммерческую тайну Общества (если необходимо);
- соблюдать порядок работы и меры по защите ставших ему известными сведений конфиденциального характера;
- немедленно, в письменной форме, информировать Директора по режиму и

экономической безопасности либо лицо, его замещающее, руководителя структурного подразделения:

- о попытках несанкционированного доступа к информационным ресурсам и сведениям, составляющим коммерческую тайну Общества, и персональным данным;
- о попытках подкупа, угроз, шантажа другими лицами с целью получения доступа к конфиденциальной информации;

- немедленно представлять Директору по режиму и экономической безопасности либо лицу, его замещающему, руководителю структурного подразделения письменные объяснения о допущенных личных нарушениях установленного порядка работы, учета и хранения документов с ИОЗТ и машинных съемных носителей информации, а также о фактах их утраты, передачи другим лицам, в том числе случайной;
- строго соблюдать правила работы с носителями ИОЗТ Общества, порядок их учета и хранения, обеспечивать в процессе работы сохранность сведений, содержащихся в них от посторонних лиц;
- знакомиться только с теми сведениями, к которым получен доступ в связи с исполнением своих трудовых обязанностей.

5.8.2. Работнику, допущенному к работе с ИОЗТ, запрещается:

- передавать без разрешения руководителя структурного подразделения сведения конфиденциального характера и документы (в устной форме, по телефону, на бумажных и машинных носителях, в электронной виде и т.д.) другим лицам;
- использовать ИОЗТ Общества в открытой переписке, статьях и выступлениях, а также в личных интересах;
- передавать по незащищенным техническим каналам связи, в том числе сообщать (обсуждать) по телефону сведения конфиденциального характера;
- снимать копии с документов, содержащих ИОЗТ или производить выписки из них без разрешения руководителя структурного подразделения;
- копировать ИОЗТ Общества и хранить ее на машинных съемных носителях информации, а также использовать различные технические средства, способные накапливать и хранить информацию в электронном виде (фото, видео и звукозаписывающую аппаратуру, сотовые телефоны и т.п.), за исключением случаев, описанных в Инструкциях;
- выполнять работы с ИОЗТ вне служебных помещений (помещений, где размещены подразделения Общества) без разрешения руководителя структурного подразделения;
- выносить из служебных помещений документы и машинные носители с ИОЗТ без разрешения руководителя структурного подразделения.

6. Обязанности руководителей структурных подразделений Общества по обеспечению режима конфиденциальности.

Руководители структурных подразделений отвечают за обеспечение режима конфиденциальности, они обязаны:

- вносить предложения на внесение (исключение) в Перечень сведений, составляющих коммерческую тайну Общества;
- организовать в подчиненных подразделениях работу по обеспечению сохранения в тайне ИОЗТ, анализировать состояние этой работы, принимать меры по предупреждению нарушений режима конфиденциальности;
- определять права и полномочия (копирование, редактирование, уничтожение и т.п) работников своего и других подразделений по доступу к ИОЗТ Общества, в том числе в имеющихся и создаваемых базах данных, вести учет предоставленного доступа, вносить соответствующие изменения и дополнения в должностные инструкции подчиненных работников;
- контролировать состояние режима конфиденциальности в своем подразделении,

направлять предложения по его совершенствованию в ДРиЭБ;
- организовывать обучение сотрудников своего подразделения порядку и правилам обращения с ИОЗТ Общества;
- организовать и контролировать в соответствии с Инструкцией учет, хранение, уничтожение документов и машинных носителей с ИОЗТ;
- не реже одного раза в квартал проверять наличие документов и зарегистрированных машинных носителей с ИОЗТ.

7. Ответственность за нарушение режима конфиденциальности.

7.1.1. Работники Общества несут персональную ответственность за нарушение режима конфиденциальности, установленного в Обществе.

7.1.2. Нарушение режима конфиденциальности, приведшее или способное привести к разглашению конфиденциальной информации, является чрезвычайным происшествием и влечет за собой последствия, предусмотренные подписанным работником Обязательством и действующим законодательством РФ.

7.1.3. По всем фактам нарушений режима конфиденциальности должны быть проведены расследования, в ходе которых определен круг лиц, виновных в этих нарушениях и причастных к ним, а также причины и условия, способствовавшие совершению данных нарушений, и приняты соответствующие меры. Для этого:
- приказом Генерального директора создается комиссия с включением в нее представителя ДРиЭБ, которая в срок не более 15 календарных дней со дня обнаружения факта нарушения проводит расследование и представляет материалы этого расследования Генеральному директору Общества;
- одновременно с работой комиссии руководителями структурных подразделений должны быть приняты меры по локализации отрицательных последствий от данного нарушения;
- на основании результатов проведенного расследования Генеральный директор Общества принимает решение о применении к виновным лицам мер материальной и/или иной ответственности в порядке, предусмотренном действующим законодательством РФ.

7.1.4. Виновные в нарушении режима конфиденциальности, повлекшем (способном повлечь) за собой разглашение ИОЗТ, в соответствии с законодательством РФ могут быть привлечены к дисциплинарной, административной или уголовной ответственности.

Приложение:

1. Перечень Документов, использованных при разработке Положения на 1 л. В 1 экз.
2. Форма договора о конфиденциальности на 3 л. в 1 экз.
3. Обязательство о неразглашении конфиденциальной информации ОАО «ФИРМА» на 2 л. в 1 экз.
4. Лист согласования Положения на 1 л. в 1 экз.

Директор по режиму и экономической безопасности ОАО «ФИРМА» **Ф.И.О.**

Приложение № 1
к Положению о защите информации,
содержащей сведения конфиденциального
характера в ОАО «ФИРМА»
(на одном листе)

Документы, использованные при разработке Положения:

1. Гражданский кодекс РФ (часть четвертая) от 18.12.2006 г. № 230-ФЗ.
2. Федеральный закон РФ № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон РФ № 98-ФЗ от 29.07.2004 г. «О коммерческой тайне».
4. Федеральный закон РФ № 152-ФЗ от 27.07.2006 г. «О персональных данных».
5. Федеральный закон РФ № 208-ФЗ от 26.12.1995 г. «Об акционерных обществах».
6. Постановление правительства РФ № 781 от 17.11.2007 г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
7. Постановление правительства РСФСР № 35 от 05.12.1991 г. «О перечне сведений, которые не могут составлять коммерческую тайну".
8. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».
9. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
10. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
11. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».
12. Указ Президента РФ №188 от 06.03.1997 года «Об утверждении перечня сведений конфиденциального характера».

Приложение № 2
к Положению о защите информации,
содержащей сведения конфиденциального
характера в ОАО «ФИРМА»
(на трех листах)

ДОГОВОР
о конфиденциальности

г. _____ «__ » _____ 201_ г.
(место составления договора)

ОАО «ФИРМА», именуемое в дальнейшем «Заказчик», в лице _____, действующего на основании _____, с одной стороны, и _____, именуемое в дальнейшем «Исполнитель», в лице _____, действующего на основании _____,
с другой стороны, вместе именуемые «Стороны», а по отдельности «Сторона», заключили настоящий Договор о нижеследующем.

1. Предмет Договора

1.1. В целях обеспечения режима конфиденциальности при проведении работ в соответствии с договором № _____ от _____, Стороны заключили настоящий Договор о порядке предоставления доступа и условиях использования информации, составляющей информацию конфиденциального характера Заказчика.

1.2. В рамках настоящего Договора Стороны относят к категории «Конфиденциальная информация» информацию, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств - на материальных объектах (носителях), в которых сведения находят свое отображение в виде символов, образов, сигналов, технических решений и процессов):

- _____
  _____
- _____
  _____
- _____
  _____
- _____
  _____

1.3. Носители информации, должны иметь гриф -

«КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ»
№ ____ от «___» _____ 201_г.
ОАО«ФИРМА»
Индекс, Город, Улица, Дом.
Телефоны:

1.4. Гриф может быть выполнен в виде надписи на документе или штампа с приложением

печати и подписи уполномоченного лица.

2. Права и обязанности Сторон

2.1 Стороны признают, что конфиденциальная информация и все права на обладание ею, или в отношении нее, доступ к которой получен Исполнителем в ходе выполнения обязательств по договору № _____ от _____, полученная Исполнителем, либо возвращенная Заказчику в первоначальном виде, или в виде результата работ, принадлежат Заказчику – правообладателю информации.

2.2 Исполнитель обязуется не разглашать и не раскрывать прямо или косвенно в какой-либо форме и какими-либо средствами предоставленную конфиденциальную информацию в целом или ее часть третьим лицам, не копировать или как-либо иначе воспроизводить ее полностью или частично в целях передачи третьей стороне без предварительного письменного согласования с Заказчиком.

2.3 Исполнитель, получая доступ к конфиденциальной информации имеет право раскрывать ее или предоставлять доступ к ней/или ее части своим сотрудникам, а также другим лицам, привлеченным им для исполнения обязательств по договору № _____ от _____, только в том объеме, в каком это необходимо для выполнения обязательств перед Заказчиком. Доступ к данной информации может быть предоставлен указанным в настоящем пункте лицам при условии, что до ее раскрытия и/или предоставления, Исполнитель получит от своих сотрудников и/или иных лиц, привлеченных Исполнителем к исполнению своих обязательств по договору № _____ от _____, обязательства по сохранению в тайне конфиденциальной информации.

2.4 Передача или предоставление доступа к конфиденциальной информации ни в коем случае не подразумевает и не означает передачу или согласие на передачу Исполнителю каких-либо лицензий или иных прав.

2.5 Исполнитель обязуется сообщать Заказчику обо всех событиях, которые могут повлечь за собой нарушение режима использования конфиденциальной информации и разглашения ее третьей стороне.

2.6 Заказчик в целях обеспечения контроля над выполнением условий настоящего договора имеет право требовать от представителей Исполнителя надлежащее исполнение обязательств при осуществлении доступа к сведениям (информационным ресурсам) Заказчика, содержащим информацию конфиденциального характера.

3. **Ответственность Сторон**

3.1. За нарушение положений, предусмотренных в Статье 2 настоящего Договора, виновная Сторона несет ответственность в полном объеме в соответствии с действующим законодательством РФ.

4. Прочие условия

4.1. Настоящий Договор вступает в силу с момента его подписания уполномоченными представителями Сторон и действует в течение трёх лет после окончания исполнения сторонами обязательств по договору № _____ от _____.

4.3. Все изменения и дополнения к настоящему Договору действительны, если они совершены в письменной форме и подписаны уполномоченными представителями Сторон.

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

4.5. Все споры и разногласия, связанные с исполнением настоящего Договора или в связи с ним. Стороны будут решать путем переговоров. В случае не достижения согласия по спорному

вопросу в течение тридцати дней с момента начала переговоров спор может быть передан заинтересованной Стороной на рассмотрение в Арбитражный суд Города и\или области.

4.6 Конфиденциальная информация может быть предоставлена соответствующим государственным органам по письменному запросу для осуществления полномочий по контролю и надзору, предоставленных им законом.

5. Адреса и реквизиты Сторон

Заказчик:
Адрес:_____
_____
ИНН:_____
р/с:_____
_____

ОКПО:_____
ОКОНХ:_____

Исполнитель:
Адрес:_____
_____
ИНН:_____
р/с:_____
_____

ОКПО:_____
ОКОНХ:_____

От Заказчика:

_____
_____
_____
_____
_____

«___» _____201_ г.

От исполнителя:

_____
_____
_____
_____
_____

«___» _____201_ г.

Приложение № 3
к Положению о защите информации,
содержащей сведения конфиденциального
характера в ОАО «ФИРМА»
(на двух листах)

ОБЯЗАТЕЛЬСТВО
о неразглашении охраняемой законом тайны
(дата прописью, место составления)

Я, _____, в качестве
(фамилия, имя, отчество)

работника ОАО «ФИРМА» в период трудовых отношений с предприятием (или его правопреемником) и в течение 3 (Трёх) лет после их окончания,
в соответствии с п. _____ трудового договора №___ от «___»_____ года, заключенного между мной _____ и ОАО «ФИРМА» (далее Общество), а также требованиями Положения о защите информации, содержащей сведения конфиденциального характера в ОАО «ФИРМА», утверждённого Приказом Генерального директора № ___ от «___»_____ 201_ года,

ОБЯЗУЮСЬ:

1) не разглашать сведения, составляющие охраняемую законом тайну, а именно:

- коммерческую тайну предприятия, согласно п.п. № (указать пункты перечня) Перечня сведений, составляющих коммерческую тайну Общества, утверждённого Приказом Генерального директора Общества № ____ от «____»_____ 201_года;
- персональные данные других работников согласно п.п. № Инструкции по обработке персональных данных Общества, утверждённой Приказом Генерального директора Общества № ____ от «____»_____ 201_ года,

которые мне доверены и стали известны в связи с исполнением трудовых обязанностей;

2) не передавать сведения лицам, не допущенным к получению ИОЗТ, в устной, письменной, электронной или иной форме и не раскрывать публично сведения, составляющие охраняемую законом тайну (государственную тайну, коммерческую тайну предприятия), персональные данные другого работника, без согласия предприятия;

3) выполнять относящиеся ко мне требования приказов, инструкций и положений по обеспечению сохранности охраняемой законом тайны (государственной тайны, коммерческой тайны предприятия), персональные данные другого работника;

4) в случае попытки посторонних лиц получить от меня сведения, составляющие охраняемую законом тайну (государственную тайну, коммерческую тайну предприятия), персональные данные другого работника немедленно сообщить _____
_____;
(должностное лицо или подразделение предприятия)

5) немедленно сообщать Директору по режиму и экономической безопасности и руководителю структурного подразделения об утрате или недостаче носителей с информацией, содержащей охраняемую законом тайну, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов, печатей и о других фактах, которые могут привести к

разглашению такой информации, а также о причинах возможной утечки (несанкционированного доступа к ней).

6) сохранять коммерческую тайну тех предприятий, с которыми имеются деловые отношения предприятия;

7) не использовать знание коммерческой тайны предприятия для занятий любой деятельностью, которая в качестве конкурентного действия может нанести ущерб предприятию;

8) в случае моего увольнения или перевода на другую должность, все носители охраняемой законом тайны (государственной тайны, коммерческой тайны предприятия), персональные данные другого работника предприятия (а именно, рукописи, черновики, чертежи, магнитные ленты, перфокарты, перфоленты, диски, флешнакопители, дискеты, распечатки на принтерах, кино-, фотонегативы и позитивы, модели, материалы, изделия и пр.), которые находились в моем распоряжении в связи с выполнением мною трудовых обязанностей во время работы на предприятии, передать руководителю структурного подразделения или в Дирекцию по режиму и экономической безопасности;

9) знакомиться только с теми сведениями, содержащими охраняемую законом тайну (государственную тайну, коммерческую тайну предприятия), персональные данные другого работника предприятия, к которым получен доступ в связи с исполнением трудовых обязанностей.

Я согласен с тем, что руководство Общества или уполномоченные им лица имеют право осуществлять контроль над соблюдением мною установленного порядка обработки средствами вычислительной техники и передачи по техническим каналам передачи данных и связи информации, содержащей охраняемую законом тайну, представленной в электронном виде.

Я предупрежден, что в случае невыполнения любого из пунктов 1, 2, 3, 4, 5, 6, 8 настоящего обязательства могу быть уволен предприятия в соответствии с подп. в п. 6 ст. 81 ТК РФ.

До моего сведения также доведены с разъяснениями соответствующие положения по обеспечению сохранности охраняемой законом тайны (государственной тайны, коммерческой тайны предприятия), персональные данные другого работника, указанные в настоящем обязательстве, а именно _____ *(перечислить).*

Мне известно, что нарушение этих положений может повлечь дисциплинарную, уголовную, административную, гражданско-правовую или иную ответственность, предусмотренную действующим законодательством Российской Федерации, в виде дисциплинарного взыскания, лишения свободы, денежного штрафа, обязанности по возмещению ущерба предприятию (убытков, упущенной выгоды и морального ущерба) и других наказаний.

«___»_____ года
(дата)

_____
(должность, подпись, Ф.И.О.)

Один экземпляр обязательства получил «___»_____ года

_____
(подпись)

Настоящее Обязательство составлено в двух экземплярах, один из которых передан работнику, один хранится в личном деле работника.

_____
(подпись, фамилия и инициалы представителя администрации и дата)

Приложение № 4
к Положению о защите информации,
содержащей сведения конфиденциального
характера в ОАО «ФИРМА»
(на одном листе)

Лист согласования
Положения о защите информации, содержащей
сведения конфиденциального характера в
ОАО «ФИРМА»

№№ п/п	**Должность**	**Подпись**	**Фамилия, инициалы**	**Дата**
1	Директор по эксплуатации		Ф.И.О.	
1	Директор по экономике и финансам		Ф.И.О.	
2	Директор по персоналу и общим вопросам		Ф.И.О.	
3	Директор по информационным технологиям		Ф.И.О.	
4	Директор по правовым и корпоративным вопросам		Ф.И.О.	
5	Директор по режиму и экономической безопасности		Ф.И.О.	
6	Начальник правового управления		Ф.И.О.	
7	Начальник протокольного отдела		Ф.И.О.	