

Краевое государственное автономное стационарное учреждение социальной защиты «Мильковский дом-интернат малой вместимости для граждан пожилого возраста и инвалидов»

У Т В Е Р Ж Д А Ю

Директор КГАУ

«Мильковский дом-интернат»

Г.А.Зубкова

«03» июня 2019 г



ПОЛОЖЕНИЕ

О конфиденциальной информации

от 03 июня 2019г

п. Атласово

И. Назначение

1.1. Настоящее Положение о конфиденциальной информации КГАУ «Мильковский дом-интернат» (далее – Положение) определяет перечень конфиденциальной информации, обрабатываемой в КГАУ «Мильковский дом-интернат» (далее – Учреждение), регламентирует оборот в Учреждении документов, содержащих информацию ограниченного доступа, не относящуюся к государственной тайне, в соответствии с требованиями и принципами, установленными действующим законодательством.

1.2. Настоящее Положение определяет общие требования, предъявляемые к регистрации, учёту, оформлению, тиражированию, хранению, использованию, уничтожению, перерегистрации конфиденциальных документов и других материальных носителей информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, а также устанавливает порядок доступа к указанной информации.

II. Область применения

2.1. Выполнение требований Положения является обязательным для сотрудников Учреждения, сотрудников иных органов и организаций, а также сотрудников надзорно-контрольных органов, получивших в установленном порядке доступ к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности.

2.2. Отнесение информации к разряду конфиденциальной производится на основании приказа Учреждения с учетом требований законодательства.

2.3. Настоящее Положение используется совместно с Порядком обращения с конфиденциальной информацией и средствами криптографической защиты в КГАУ «Мильковский дом-интернат», утвержденным приказом.

III. Нормативные ссылки

3.1. Настоящее Положение разработано в соответствии со следующими нормативными правовыми актами:

- статьями 23 и 24 Конституции Российской Федерации;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

- ст.6 Федерального закона от 28.12.2013 № 442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации»;
- главой 14 Трудового кодекса Российской Федерации;
- Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- ГОСТ Р 6.30-2003. Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов;
- ГОСТ Р 51141-98. Делопроизводство и архивное дело. Термины и определения;
- ГОСТ Р ИСО 15489-1-2007. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования;
- Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, утвержденным приказом Министерства культуры Российской Федерации от 25.08.2010 № 558 (зарегистрировано в Минюсте РФ 08.09.2010, регистрационный № 18380);
- Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 № 17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный № 28608).

IV. Термины, обозначения и сокращения

4.1. В настоящем Положении используются следующие термины, обозначения и сокращения:

4.1.1. **Безопасность информации [данных]** - 1) состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность; 2) состояние защищенности информации, характеризующееся способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

4.1.2. **Государственная тайна** - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации, отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации, регулируются Законом РФ от 21.07.1993 №5485-1 (ред. от 21.12.2013) «О государственной тайне».

4.1.3. **Гриф конфиденциальности** - гриф ограниченного доступа, проставляемый на конфиденциальных документах в соответствии с требованиями настоящего Положения.

4.1.4. **Должностное лицо** – сотрудник Учреждения, правомочный от имени Учреждения исполнять определенные, предусмотренные должностными обязанностями действия.

4.1.5. **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.

4.1.6. **Информация** - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

4.1.7. **Информация, в отношении которой установлено требование об обеспечении ее конфиденциальности (конфиденциальная информация, конфиденциальные сведения)** –

1) информация, для которой установлен специальный режим сбора, хранения, обработки, распространения и использования, доступ к которым ограничен в соответствии с федеральным законом (за исключением сведений, составляющих государственную тайну) и определен внутренними организационно-распорядительными актами, устанавливающими разрешительную систему допуска к указанной информации;

2) информация, указанная в Перечне конфиденциальной информации КГАУ «Миловский дом-интернат», утвержденном приказом Учреждения.

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

4.1.9. **Конфиденциальный документ** - информация, зафиксированная на материальном носителе, содержащая коммерческую, служебную или иную охраняемую законом тайну, с реквизитами, позволяющими ее идентифицировать и обеспечивать защиту, доступ к которой ограничивается федеральными законами, а также ее обладателем.

4.1.10. **Машинные носители информации (далее: МНИ)** - физическое устройство (дискета, e-Token, смарт-карта и т.д.), предназначенное для хранения информации в электронной форме.

4.1.11. **Обладатель информации, информационных ресурсов, информационных систем, технологий и средств их обеспечения** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

4.1.12. **Перечень Глав архива** – «Перечень типовых документов, образующихся в деятельности госкомитетов, министерств, ведомств и других учреждений, организаций, предприятий, с указанием сроков хранения» (утв. Глав архивом СССР 15.08.1988).

4.1.13. **Перечень Минкультуры** - «Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержденный приказом Министерства культуры Российской Федерации от 25.08.2010 №558 (зарегистрировано в Минюсте РФ 08.09.2010 регистрационный № 18380).

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

4.1.15. **Пользователь (потребитель) информации** –

1) субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею;

2) сотрудник Учреждения или иное лицо, допущенное в установленном порядке к работе с конфиденциальной информацией Учреждения.

4.1.16. **Служебная тайна** – вид конфиденциальной информации, служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами.

4.2. В настоящем Положении используются следующие сокращения:

4.2.1. **ИСПДн**- информационная система персональных данных;

4.2.2. **МНИ**- машинные носители информации;

4.2.3. **ПДЭК**- Постоянно действующая экспертная комиссия;

V. Конфиденциальная информация и ее отношение к различным видам тайн

6.1. Частью 3 статьи 5 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» определено, что информация в зависимости от порядка ее предоставления или распространения подразделяется на;

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

6.2. Перечнем сведений конфиденциального характера, утвержденного Указом Президента Российской Федерации от 06.03.97 № 188 «Об утверждении Перечня сведений конфиденциального характера» определено, что к конфиденциальной информации относятся:

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

- сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с федеральными законами от 20.04.1995 №45-ФЗ "О государственной защите судей, должностных лиц правоохранительных и контролирующих органов" и от 20.08.2004 №119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства", другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну;

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

- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

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

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

- сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 02.10.2007 №229-ФЗ «Об исполнительном производстве».

6.3. Таким образом, все виды тайн, не являющиеся информацией, относимой к государственной тайне, являются частным проявлением более широкого понятия «конфиденциальная информация» или «информация, в отношении которой установлено требование об обеспечении ее конфиденциальности».

6.4. Одна и та же по содержанию информация в зависимости от обстоятельств может находиться под защитой как одного, так и нескольких правовых режимов защиты.

Кроме того, одна и та же информация в зависимости от отношения к ее обладателю может выступать как тайны различного вида.

Например: персональные данные являются одним из видов информации, в отношении которой установлено требование об обеспечении ее конфиденциальности. При этом, по отношению к субъекту персональных данных эта информация может являться личной тайной, а по отношению к государственному или муниципальному служащему, обрабатывающему персональные данные иных субъектов на законном основании, эта информация выступает в виде служебной тайны, а для врачей - в виде врачебной тайны, адвокатов - в виде адвокатской тайны, для священнослужителя - тайной исповеди и т.д.

6.5. В соответствии с Постановлением Правительства РФ от 03.11.1994 №1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» и рядом нормативных правовых актов субъектов Российской Федерации, принятых по образцу данного постановления, в органах государственной власти и местного самоуправления используется гриф конфиденциальности «Для служебного пользования» («ДСП»). Использование грифа «ДСП» в коммерческих организациях и иных учреждениях¹ не принято².

6.6. В ряде коммерческих организаций в соответствии с Федеральным законом от 29.07.2004 №98-ФЗ «О коммерческой тайне» и Указом Президента Российской Федерации от 06.03.97 № 188 «Об утверждении Перечня сведений конфиденциального характера» используется гриф ограниченного доступа «Коммерческая тайна».

6.7. В других организациях и учреждениях в соответствии с Перечнем сведений конфиденциального характера, утвержденного Указом Президента Российской Федерации от 06.03.97 № 188, Федеральным законом от 08.02.1998 №14-ФЗ «Об обществах с ограниченной ответственностью», Федеральным законом от 25.04.2002 № 40-ФЗ "Об обязательном страховании гражданской ответственности владельцев транспортных средств» и многих других принят гриф ограниченного доступа **Конфиденциально**.

6.8. Учреждение, являясь подведомственным Министерству социальной защиты населения Камчатского края учреждением, использует гриф ограниченного доступа **«Конфиденциально»**.

6.9. Из сказанного выше следует, что:

6.9.1. при поступлении в Учреждение из органов государственной власти, местного самоуправления, других организаций или учреждений документов, содержащих информацию ограниченного доступа, не относящуюся к сведениям, составляющим государственную тайну, и имеющих гриф конфиденциальности «Конфиденциально», «Для служебного пользования», «Коммерческая тайна», «Врачебная тайна» или др., регистрация и учет поступивших документов должен проводиться в соответствии с настоящим Положением;

¹ Включая государственные и муниципальные учреждения.

² Грифом «Для служебного пользования» помечаются документы, содержащие служебную тайну. В соответствии с Указом Президента Российской Федерации от 06.03.97 № 188 (ред. от 13.07.2015) служебная тайна определяется как служебные сведения ограниченного доступа **органов государственной власти**. В п.3.1.4. ГОСТ Р 51583-2000 Порядок создания автоматизированных систем в защищенном исполнении и п.3.1.2. ГОСТ Р 51624-2000 «АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ» определено: «Служебная тайна - защищаемая по закону конфиденциальная информация, ставшая известной в **государственных органах и органах местного самоуправления** только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости».

6.9.2. термины: «информация, в отношении которой установлено требование об обеспечении ее конфиденциальности»³, «конфиденциальная информация»⁴, «информации ограниченного доступа, не содержащая сведения, составляющие государственную тайну»⁵ определяют одно и то же понятие;

6.9.3. термины «конфиденциальная информация» и «служебная тайна» в отношении информации ограниченного доступа, не относящейся к государственной тайне и находящейся в распоряжении сотрудников Учреждения на законном основании, определяют одно и то же понятие, и не является служебной тайной как таковой.

VI. Режим ограниченного доступа к конфиденциальной информации

7.1. Режим ограниченного доступа к конфиденциальной информации Учреждения предполагает:

- 7.1.1. утверждение Перечня сведений конфиденциального характера Учреждения;
- 7.1.2. установление единого порядка допуска к конфиденциальной информации;
- 7.1.3. установление единого порядка обращения в Учреждении конфиденциальных документов (создание, регистрация, прием, отправление, хранение, уничтожение);
- 7.1.4. установление разрешительной системы допуска к информационным ресурсам информационных систем.

VII. Организация допуска к конфиденциальной информации

8.1. Учёт лиц, получивших доступ к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, и лиц, которым такая информация была предоставлена или передана

8.1.1. В Учреждении ведется учет:

- сотрудников Учреждения, получивших доступ к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, а также информации, к которой они получили доступ в соответствии с Перечнем должностей учреждения, допущенных к работе с конфиденциальной информацией, утвержденным приказом Учреждения;
- должностных лиц органов государственной власти, иных государственных органов, получивших доступ к находящейся в ведении Учреждения информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, в период проведения ими проверок в Журнале проверок;
- на специалиста по кадрам возлагаются функции по организации и ведению конфиденциального делопроизводства.

8.2. Порядок допуска к конфиденциальной информации сотрудников Учреждения

³ Используется в терминологии Федерального закона от 11.07.2011 №200-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "Об информации, информационных технологиях и о защите информации".

⁴ Используется в терминологии:

- Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.2002 № 282;
- приказа ФАПСИ РФ от 13.06.2001 № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (Бюллетень нормативных актов федеральных органов исполнительной власти, 2001. – № 34) и других документов Регуляторов.

⁵ Используется в терминологии приказа ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (Зарегистрировано в Минюсте России 31.05.2013 №28608).

8.2.1. Допуск сотрудников Учреждения к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, осуществляется на основании:

8.2.1.1. наличия должности сотрудника, допускаемого к конфиденциальной информации, в Перечне должностей сотрудников, замещение которых предусматривает допуск сотрудника к конфиденциальной информации Учреждения, утвержденного приказом Учреждения;

8.2.1.2. изучения сотрудником, допускаемым к указанной информации, требований настоящего Положения, Положения о разрешительной системе допуска пользователей к информационным системам Учреждения, в которых обрабатывается конфиденциальная информация и его росписи в листах ознакомления;

8.2.1.3. получение от сотрудника, допускаемого к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, Обязательства сотрудника о неразглашении конфиденциальной информации Учреждения (Приложение №1 к настоящему Положению).

8.2.2. Руководители структурных подразделений Учреждения осуществляют контроль допуска подчиненных сотрудников к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности.

8.2.3. Процедура допуска к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности:

8.2.3.1. Специалист по кадрам:

8.2.3.1.1. организует изучение положений и требований сотрудниками Учреждения, допускаемыми к конфиденциальной информации, под подпись в листах ознакомления с настоящим Положением и Положением о разрешительной системе допуска пользователей к информационным системам Учреждения, в которых обрабатывается конфиденциальная информация;

8.2.3.1.2. обеспечивает хранение листов ознакомления с настоящим Положением и Положением о разрешительной системе допуска пользователей к информационным системам Учреждения, в которых обрабатывается конфиденциальная информация;

8.2.3.1.3. принимает от сотрудников Учреждения Обязательства о неразглашении конфиденциальной информации, не содержащей сведений, составляющих государственную тайну (Приложение №1 к настоящему Положению).

VIII. Порядок обращения в Учреждении конфиденциальных документов

9.1. Порядок подготовки, оформления документов, учета и хранения материальных носителей конфиденциальной информации

9.1.1. Если форма документа утверждена нормативным актом органа государственной власти или местного самоуправления и при этом указанная форма документа не предусматривает проставления грифа ограничения доступа (конфиденциальности), но сам документ содержит сведения, отнесенные к конфиденциальной информации в соответствии с законодательством или Перечнем сведений конфиденциального характера Учреждения, то гриф конфиденциальности на указанном документе не ставится, а хранение, пересылка и другие действия с указанным документом осуществляются в соответствии с настоящим Положением.

Например:

9.1.1.1. Форма трудовой книжки утверждена Постановлением Правительства РФ от 16.04.2003 №225 «О трудовых книжках» (вместе с «Правилами ведения и хранения трудовых книжек, изготовления бланков трудовой книжки и обеспечения ими работодателей»). Данная форма не содержит грифа конфиденциальности, но при заполнении трудовой книжки в нее вносятся персональные данные, отнесенные к

конфиденциальной информации в соответствии с Указом Президента РФ от 06.03.1997 №188 «Об утверждении Перечня сведений конфиденциального характера» Хранение трудовой книжки должно производиться в соответствии с правилами хранения материальных носителей конфиденциальной информации.

9.1.2. Регистрация конфиденциальных документов производится в специальных журналах, форма и перечень которых установлен Порядком обращения с конфиденциальной информацией и средствами криптографической защиты в КГАУ «Мильковский дом-интернат», утвержденным приказом Учреждения.

9.1.3. Сотрудник Учреждения, ответственный за ведение делопроизводства или хранение конфиденциальных документов, несет персональную ответственность за их сохранность и выдачу только лицам, допущенным к конфиденциальной информации в порядке раздела VII настоящего Положения. Допуск к конфиденциальной информации иных лиц возможен только после письменного указания директора учреждения.

9.1.4. Места и сроки хранения конфиденциальных документов, предусмотрены приказом Учреждения «Об утверждении сроков и мест хранения материальных носителей персональных данных» и должны предусматривать раздельное хранение конфиденциальных и не конфиденциальных документов. Возможно совместное хранение в конфиденциальном деле конфиденциальных и не конфиденциальных документов, объединенных общей темой. Ознакомление лица, не имеющего допуска к конфиденциальной информации, с не конфиденциальным документом, хранящимся в конфиденциальном деле, должен исключить возможность его ознакомления с иными конфиденциальными документами указанного дела.

9.1.5. Хранение носителей конфиденциальной информации осуществляется в местах, исключающих несанкционированный доступ к ним посторонних лиц. При этом:

9.1.5.1. трудовые книжки хранятся в сейфах (металлических шкафах) как бланки строгой отчетности⁶;

9.1.5.2. съемные носители конфиденциальной информации в незашифрованном с использованием средств криптографической защиты информации (далее-СКЗИ) виде хранятся в сейфах (металлических шкафах)

9.1.5.3. учет указанных сейфов или металлических шкафов для носителей конфиденциальной информации и СКЗИ ведется лицом, назначенным приказом директора Учреждения, в соответствии с Порядком обращения с конфиденциальной информацией и средствами криптографической защиты в КГАУ «Мильковский дом-интернат», утвержденным приказом Учреждения, в журнале учета сейфов и хранилищ;

9.1.5.4. дубликаты ключей от хранилищ со СКЗИ хранятся в сейфе (хранилище) директора учреждения в соответствии с Порядком обращения с конфиденциальной информацией и средствами криптографической защиты в КГАУ «Мильковский дом-интернат», утвержденным приказом Учреждения.

9.1.6. Снятие ограничения доступа к конфиденциальным документам производится по акту Постоянно действующей экспертной комиссии, утвержденному директором Учреждения.

9.2. Порядок предоставления конфиденциальной информации Учреждения третьим лицам

9.2.1. По общему правилу предоставление конфиденциальной информации Учреждения третьим лицам возможно только на законном основании по указанию директора Учреждения, несущего персональную ответственность за принятое решение.

9.2.2. Предоставление персональных данных как вида конфиденциальной информации имеет ряд особенностей:

⁶ См.п.42 Правил ведения и хранения трудовых книжек, изготовления бланков трудовой книжки и обеспечения ими работодателей, утвержденных Постановлением Правительства РФ от 16.04.2003 №225.

9.2.2.1. операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

9.2.2.2. В соответствии с федеральным законодательством Учреждение обязано предоставлять персональные данные субъектов следующим органам (организациям) или их должностным лицам:

9.2.2.2.1. по мотивированному запросу прокурора, руководителя следственного органа, следователя, органа дознания и дознавателя, предъявленному в пределах их полномочий, установленных Уголовно-процессуальным кодексом Российской Федерации";

9.2.2.2.2. военным комиссариатам – сведения о воинском учете сотрудников (категория запаса, воинское звание, состав (профиль), полное кодовое обозначение ВУС, категория годности к военной службе, наименование комиссариата по месту жительства, воинский учет (общий, специальный);

9.2.2.2.3. налоговым органам – фамилия, имя, отчество, дата и место рождения сотрудника; его оклад; произведенные сотруднику начисления и выплаты, данные о заработной плате, номер лицевого счета в банке; табельный номер, суммарный доход с начала года;

9.2.2.2.4. территориальным органам Пенсионного фонда РФ – номер страхового свидетельства государственного пенсионного страхования сотрудника, стаж для расчета страховой части пенсионных накоплений сотруднику;

9.2.2.2.5. участникам межведомственного взаимодействия в пределах их полномочий, установленных действующим законодательством;

9.2.2.2.6. иным органам, организациям и физическим лицам в соответствии с действующим законодательством.

9.3. Уничтожение документов, содержащих конфиденциальную информацию

9.3.1. Уничтожение документов, содержащих конфиденциальную информацию производится по акту в соответствии с Порядком обращения с конфиденциальной информацией и средствами криптографической защиты в КГАУ «Мильковский дом-интернат», утвержденным приказом Учреждения.

9.3.2. Отобранные к уничтожению документы измельчаются механическим способом до степени, исключающей возможность прочтения текста, или сжигаются в печи до золы.

9.3.3. Хранение конфиденциальной информации в не обезличенном виде на магнитных носителях не допускается.

9.3.4. В целях гарантированного уничтожения файлов и затирания остаточной информации на магнитном носителе либо уничтожения носителей механическим способом привлекается ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных.

9.3.5. Факт уничтожения конфиденциальных материалов оформляется соответствующим актом, утверждаемым директором Учреждения.

9.3.6. По факту утраты конфиденциальных документов, дел и других материалов или разглашения сведений, содержащихся в этих материалах, проводится служебная проверка и составляется заключение служебной проверки, которая утверждается директором Учреждения⁷.

⁷ Исполняется в соответствии с:

- п.7 Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001. № 152 (Бюллетень нормативных актов федеральных органов исполнительной власти, 2001. № 34);
- п.2.3. и п. 3.24. «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений,

IX. Ответственность и полномочия персонала

10.1. Ответственность персонала

10.1.1. Ответственность за несоблюдение требований, установленных настоящим Положением, несут:

– ответственный за организацию обработки персональных данных в Учреждении, за осуществление контроля организации допуска сотрудников Учреждения и сотрудников иных органов и организаций к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, а также за контроль поддержания установленного уровня защиты конфиденциальной информации, за организацию допуска сотрудников Учреждения к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности;

– специалист по кадрам, за организацию конфиденциального делопроизводства в Учреждении и организацию допуска сотрудников иных органов и организаций к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности;

– ответственный за защиту персональных данных в информационной системе персональных данных за осуществление защиты конфиденциальной информации в информационных системах;

– администратор локальной вычислительной сети за поддержание установленного уровня защищенности информационных систем, обрабатывающих конфиденциальную информацию;

– директор Учреждения за контроль выполнения требований настоящего Положения;

– сотрудники Учреждения и иные лица, допущенные в установленном порядке к информации, в отношении которой установлены требования об обеспечении ее конфиденциальности, за неисполнение требований настоящего Положения в части, их касающейся.

10.1.2. Руководитель, принявший решение, влияющее на защищенность информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, несет персональную ответственность за принятое решение.

10.1.3. Лица, указанные в п.9.1.1 настоящего Положения, за нарушение требований действующего законодательства и настоящего Положения несут уголовную, гражданскую, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.

10.2. Полномочия персонала

Сотрудники Учреждения имеют право выходить с предложениями к руководству Учреждения по вопросам защиты конфиденциальной информации. Изменения в настоящее Положение вносятся приказом Учреждения.

составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622;

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации,
не содержащей сведений, составляющих государственную тайну

Я, _____
(Ф.И.О. работника)

исполняющий(ая) должностные обязанности по замещаемой должности _____

(должность, наименование организации)

назначенный(ая) приказом _____
(кем назначен, наименование организации)

№ _____ от « _____ » _____ 20__ года, предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностной инструкцией (должностным регламентом) мне будет предоставлен допуск к конфиденциальной информации, не содержащей сведений, составляющих государственную тайну <1> (далее – конфиденциальные сведения), персональным данным отдельных категорий граждан <2>.

Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать<3>, не передавать и не раскрывать третьим лицам<4> конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей, за исключением случаев привлечения последних к деятельности, требующей раскрытия такой информации и только в объеме, необходимом для реализации целей и задач КГАУ «Мильковский дом-интернат» (далее – Учреждение), с письменного разрешения _____.

(руководитель, наименование организации)

2. Выполнять, относящиеся ко мне требования внутренних организационно-распорядительных актов Учреждения в части оборота, неразглашения, нераспространения и защиты конфиденциальной информации.

3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному начальнику, а также лицу, ответственному за организацию защиты информации в Учреждении.

4. Не производить преднамеренных действий, нарушающих достоверность, целостность конфиденциальной информации Учреждения.

5. Не использовать ставшие мне известными или разработанные мною конфиденциальные сведения иначе, как в интересах Учреждения и не использовать их с целью получения выгоды.

6. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений, а также соблюдать правила и меры по защите конфиденциальной информации, указанные в Порядке обращения с конфиденциальной информацией и средствами криптографической защиты информации в Учреждении и в других организационно-распорядительных правовых актах Учреждения.

7. В случае прекращения работы в Учреждении, сразу же вернуть Учреждению все документы и другие материалы, содержание которых отнесено к конфиденциальной информации, полученные мною в ходе выполнения своих служебных обязанностей.

8. После прекращения права на допуск к конфиденциальным сведениям, ставшие мне известные персональные данные не подлежат разглашению и передаче третьим лицам в течение неограниченного срока.

Я подтверждаю, что ознакомлен(а) с правилами и мерами по защите конфиденциальной информации, действующими в Учреждении и до моего сведения доведены с разъяснениями соответствующие требования Положения о конфиденциальной информации Учреждения.

Я подтверждаю, что не имею перед кем-либо никаких обязательств, которые входят в противоречие с настоящим обязательством или ограничивают мою деятельность в Учреждении.

Я предупрежден(а), что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной, административной или уголовной ответственности в соответствии с действующим законодательством.

(Ф.И.О.)

/ _____ /
(подпись)

« ____ » _____ 20 ____ г.

<1> государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации (абзац 2 статьи 2 Федерального закона «О государственной тайне»).

<2> 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 (пункт 1 статьи 3 Федерального закона «О персональных данных»).

<3> Под разглашением понимается умышленное или неумышленное (неосторожное) действие лица, приведшие к ознакомлению (оглашению) с конфиденциальными сведениями лиц, не имеющих в установленном порядке допуска к конфиденциальным сведениям.

<4> Третьи лица - лица, не имеющие в установленном порядке допуска к конфиденциальным сведениям.
