Выписка из приказа Министерства «Об утверждении Положения о конфиденциальной информации Министерства»

1. Назначение

1.1. Настоящее Положение о конфиденциальной информации в Министерстве (далее – Положение) определяет перечень конфиденциальной информации, обрабатываемой в Министерстве, регламентирует оборот в данном органе власти документов, содержащих информацию ограниченного доступа, не относящуюся к государственной тайне, в соответствии с требованиями и принципами, установленными действующим законодательством.

1.2. Перечень конфиденциальной информации может быть актуализирован по мере надобности отдельными приказами Министерства.

1.3. 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.

2. Область применения

2.1. Выполнение требований Положения является обязательным для сотрудников Министерства, 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. Относить информацию Министерства к разряду конфиденциальной может своим приказом, вносящим изменения в Перечень сведений конфиденциального характера Министерства с учетом требований законодательства[1].

3. 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»;
- главой 14 Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ;
- 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»;
- 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);
- приказа Федерального архивного агентства от 20.12.2019 № 236 «Об утверждении перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения» (зарегистрировано в Минюсте России 06.02.2020 №57449);
- приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (зарегистрировано в Минюсте России 18.08.2014 №33620).

4. Термины, обозначения и сокращения

---

[1] См.:
- ч.4 ст.6 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Указ Президента РФ от 06.03.1997 №188 "Об утверждении Перечня сведений конфиденциального характера".

–
–
–

5. Конфиденциальная информация и ее отношение к различным видам тайн

5.1. 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.

5.2. Статьей 10 Федерального закона от 20.02.1995 № 24-ФЗ было определено, что «документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную[2]».

5.3. 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».

5.4. 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».

5.5. 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[3], адвокатов - в виде адвокатской тайны[4], для священнослужителя - тайной исповеди[5] и т.д.

5.6. В соответствии с Постановлением Правительства РФ от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в

---

[2] 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" конфиденциальная информация называется «информация, в отношении которой установлено требование об обеспечении ее конфиденциальности».

[3] См. ст.13 Федерального закона от 21.11.2011 №323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации.

[4] См.: ст.8 Федерального закона от 31.05.2002 №63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации".

[5] См.: ч.7 ст.3 Федерального закона от 26.09.1997 №125-ФЗ "О свободе совести и о религиозных объединениях".

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 учреждениях[6] не принято[7].

5.7. В ряде коммерческих организаций в соответствии с Федеральным законом от 29.07.2004 №98-ФЗ «О коммерческой тайне» и Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» используется гриф ограниченного доступа «Коммерческая тайна».

5.8. В других организациях и учреждениях в соответствии с Перечнем сведений конфиденциального характера, утвержденного Указом Президента Российской Федерации от 06.03.1997 № 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**.

5.9. Министерство, являясь органом государственной власти субъекта Российской Федерации, должно использовать единый гриф ограниченного доступа **«Для служебного пользования»** или **«ДСП»**. Подведомственные Министерству учреждения, которые не являются органами государственной власти или местного самоуправления должны использовать гриф ограниченного доступа **«Конфиденциально»** или **Конф**.

5.10. Для документов, предназначенных для всех сотрудников Министерства (или их подавляющего большинства), но не предназначенных для свободной публикации в открытых источниках, возможно применение грифа ограничения доступа **«Для внутреннего пользования»**[8]. Регистрация, хранение и уничтожение указанных документов осуществляется в соответствии с правилами, установленными для конфиденциальных документов. Особый порядок допуска сотрудников Министерства к документам с грифом ограничения доступа «Для внутреннего пользования» не устанавливается, доступ сотрудников Министерства осуществляется как к неконфиденциальным документам. Порядок допуска сотрудников иных организаций при выполнении работ по государственному контракту (гражданско-правовому договору) и сотрудников надзорно- контрольных органов при проведении ими проверки осуществляется в порядке, установленном для допуска к конфиденциальной информации[9].

5.11. Из сказанного выше вытекает, что:

- при поступлении в Министерство 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 ограничения доступа **конфиденциально**, д**ля служебного пользования**, к**оммерческая тайна**, **врачебная тайна** или др., регистрация и учет поступивших документов должен проводиться в соответствии с настоящим Положением;
- термины: «информация, в отношении которой установлено требование об обеспечении ее конфиденциальности»[10], «конфиденциальная информация»[11], «информации ограниченного доступа, не содержащая сведения, составляющие государственную тайну»[12] в настоящем Положении являются синонимичными.

---

[6] Включая государственные и муниципальные учреждения.

[7] Грифом «Для служебного пользования» помечаются документы, содержащие служебную тайну. В соответствии с Указом Президента Российской Федерации от 06.03.97 № 188 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».

[8] В соответствии с частью 3 статьи 5 Федерального закона от 27 от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации" информация, содержащаяся в документах с грифом «Для внутреннего пользования» относится к информации, предоставляемой по соглашению лиц, участвующих в соответствующих отношениях.

[9] См.разд.7.3 и разд.7.4 настоящего Положения.

[10] 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".

[11] 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.

[12] 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).

6. Режим ограниченного доступа к конфиденциальной информации

6.1.Режим ограниченного доступа к конфиденциальной информации Министерства предполагает:

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

7. Организация допуска к конфиденциальной информации

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

7.1.1 В Министерстве ведётся учёт:

7.1.1.1. сотрудников Министерства, получивших доступ к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, а также информации, к которой они получили доступ;

7.1.1.2. должностных лиц органов государственной власти, иных государственных органов, получивших доступ к находящейся в ведении Министерства информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, в период проведения ими проверок либо иных мероприятий, проводимых в рамках полномочий данных органов власти, а также информации, к которой они получили доступ;

7.1.1.2. .органов государственной власти, иных государственных органов и органов местного самоуправления, которым была предоставлена в соответствии с их мотивированными требованиями (запросами) находящаяся в ведении Министерства, в отношении которой установлено требование об обеспечении ее конфиденциальности, и переданных им материалов;

7.1.1.3. контрагентов, которым в соответствии с заключёнными соглашениями о конфиденциальности в рамках государственных контрактов или гражданско- правовых договоров была передана информация, в отношении которой установлено требование об обеспечении ее конфиденциальности, и переданных им материалов, а также представителей контрагентов, получивших доступ к такой информации при выполнении работ в Министерстве;

7.1.1.4. физических лиц, получивших доступ к конфиденциальной информации Министерства в соответствии с заключенными гражданско-правовыми договорами.

7.1.1.5. Контроль соблюдения порядка учёта лиц выше указанных категорий осуществляет ответственный за организацию обработки персональных данных, а сам учёт ведется **администратором безопасности информации** Министерства в Журнале учета должностных лиц, допущенных к конфиденциальной информации Министерства.

7.2. Порядок допуска к конфиденциальной информации сотрудников Министерства

7.2.1. Допуск сотрудников Министерства к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности, определяется внутренними приказами Министерства. Сотрудник в обязательном порядке подписывает Обязательства о неразглашении конфиденциальной информации Министерства. Порядок допуска сотрудников является конфиденциальной информаций и не подлежит размещению (опубликованию) в открытых источниках информации.

7.3. Порядок допуска к конфиденциальной информации сотрудников иных организаций при выполнении работ по государственному контракту (гражданско-правовому договору)

7.3.1. Допуск к конфиденциальной информации Министерства сотрудников иных организаций при выполнении работ по гражданско-правовому договору осуществляется на основании государственного контракта или гражданско- правового договора, заключенного Министерства, в котором в обязательном порядке содержатся требования о соблюдении конфиденциальности[13]. Допускаемые к конфиденциальной информации физические лица в обязательном порядке подписывают Соглашения о неразглашении конфиденциальной информации. Дальнейший Порядок допуска физических лиц является конфиденциальной информаций и не подлежит размещению (опубликованию) в открытых источниках информации.

7.4. Порядок допуска к конфиденциальной информации сотрудников надзорно-контрольных

---

[13] В соответствии с:

- ч.3 ст.6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ст. 3 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.2 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 №21 (Зарегистрировано в Минюсте России 14.05.2013 №28375);
- п.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (Зарегистрировано в Минюсте России 31.05.2013 №28608).

органов при проведении ими проверки

7.4.1. Допуск к конфиденциальной информации Министерства сотрудников надзорно-контрольных органов при проведении ими проверки осуществляется на основании:

7.4.1.1. закона, наделяющего сотрудников указанных надзорно-контрольных органов правом получать доступ к конфиденциальной информации проверяемой организации;

7.4.1.2. приказа надзорно-контрольного органа о проведении проверки[14], где указаны фамилии, инициалы и должности лиц, назначенных для проведения проверки.

8. Порядок обращения конфиденциальных документов

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

8.1.1. Если создаваемые документы содержат информацию ограниченного доступа, указанную в Перечне сведений конфиденциального характера Министерства, исполнителем документа в правом верхнем углу проставляются гриф ограниченного доступа **«Конфиденциально» или «Конф.»**.

8.1.2. Необходимость проставления грифа ограничения доступа на документах и изданиях, содержащих конфиденциальную информацию, по общему правилу определяется исполнителем и должностным лицом, подписывающим или утверждающим документ[15]. Из этого вытекает, что при получении из иных органов и организаций документа, не имеющего гриф ограничения доступа, но реально содержащего конфиденциальную информацию, в Министерства регистрация указанного документа производится как **неконфиденциального**. В последствии, решением министра данный документ может быть перерегистрирован как конфиденциальный с грифом «Конфиденциально» или «Конф.».

8.1.3. 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 Министерства, то гриф конфиденциальности на указанном документе не ставится, а хранение, пересылка и другие действия с указанным документом осуществляются в соответствии с настоящим Положением.

8.1.4. Регистрация конфиденциальных документов производится в общем порядке с добавлением к номеру документа грифа ограничения доступа «конф.» или «Для внутреннего пользования»

8.1.5. Сотрудник Министерства, 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 7 настоящего Положения. Допуск к конфиденциальной информации иных лиц возможен только после письменного указания министра или заместителя министра, ответственного за организацию обработки персональных данных в Министерства.

8.1.6. Места и сроки хранения конфиденциальных документов определены приказами Министерства и должны предусматривать раздельное хранение конфиденциальных и неконфиденциальных документов. Возможно совместное хранение в конфиденциальном деле конфиденциальных и неконфиденциальных документов, объединенных общей темой. Порядок ознакомления лица, не имеющего допуска к конфиденциальной информации, с неконфидециальным документом, хранящимся в конфиденциальном деле, должен исключить возможность его ознакомления с иными конфиденциальными документами указанного дела.

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

8.1.7.1. трудовые книжки хранятся в сейфах (металлических шкафах) как бланки строгой отчетности;

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

8.1.7.3. учет указанных сейфов или металлических шкафов для носителей конфиденциальной информации и СКЗИ ведется администратором безопасности, в журнале учета хранилищ;

8.1.7.4. дубликаты ключей от помещений, в которых установлены или хранятся СКЗИ хранятся в опечатанном виде у администратора безопасности.

8.1.7.5. Бумажные носители конфиденциальной информации хранятся в номерных хранилищах, шкафах кабинетов контролируемой зоны Министерства, определенных внутренними приказами Министерства и снабжаются средствами контроля вскрытия.

8.1.8. Снятие ограничения доступа к конфиденциальным документам производится по акту экспертной комиссии, утвержденному министром. При этом на документе ставится отметка: «Гриф ограничения доступа снят по акту ЭК от «___»__20__г. №__».

---

[14] См.: ч.1 ст.14 Федерального закона от 26.12.2008 №294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля".

[15] См.: п.2.1 Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии, утвержденного постановлением Правительства РФ от 03.11.1994 №1233.

8.2. Порядок предоставления конфиденциальной информации третьим лицам

8.2.1. По общему правилу предоставление конфиденциальной информации Министерства края третьим лицам возможно только на законном основании по указанию министра, несущего персональную ответственность за принятое решение.

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

8.2.2.1. 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[16].

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

8.2.3.1. по мотивированному запросу прокурора, руководителя следственного органа, следователя, органа дознания и дознавателя, предъявленному в пределах их полномочий, установленных Уголовно-процессуальным кодексом Российской Федерации[17];

8.2.3.2. 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)[18];

8.2.3.3.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[19];

8.2.3.4. территориальным органам Фонда пенсионного и социального страхования РФ - номер страхового свидетельства государственного пенсионного страхования сотрудника, стаж для расчета страховой части пенсионных накоплений сотруднику[20];

8.2.3.5. участникам межведомственного взаимодействия в пределах их полномочий, установленных действующим законодательством[21].

8.3. Уничтожение документов, содержащих конфиденциальную информацию

---

[16] См.: ст.7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

[17] См.: ч.4 ст.21 Уголовно- процессуального кодекса Российской Федерации" от 18.12.2001 №174-ФЗ.

[18] В соответствии:

- ч.1 ст.4, ст.8 Федерального закона от 28.03.1998 №53-ФЗ "О воинской обязанности и военной службе";
- ст.9 Федерального закона от 26.02.1997 № 31-ФЗ "О мобилизационной подготовке и мобилизации в Российской Федерации";
- раздела III Постановления Правительства РФ от 27.11.2006 №719 "Об утверждении Положения о воинском учете";
- п/п «г» п.27 Методических рекомендаций по ведению воинского учета в организациях, утвержденных Начальником Генерального штаба Вооруженных Сил Российской Федерации - Первым заместителем Министра обороны Российской Федерации генералом армии В. Герасимовым 11.07.2017);
- постановления Госкомстата РФ от 05.01.2004 № 1 "Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты", изданного во исполнение ч.1 ст.6 Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ от 30.12.2001 №197-ФЗ.

[19] В соответствии с:

- ст.23 части первой Налогового кодекса Российской Федерации (часть первая) от 31.07.1998 №146-ФЗ;
- гл.23 части второй Налогового кодекса Российской Федерации (часть вторая) от 05.08.2000 N 117-ФЗ;
- унифицированными формами первичной учетной документации по учету труда и его оплаты, утвержденными постановлением Госкомстата РФ от 05.01.2004 №1, изданного во исполнение ч.1 ст.6 Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ от 30.12.2001 №197-ФЗ.

[20] В соответствии с:

- ч.2 ст.14 Федерального закона от 15.12.2001 №167-ФЗ "Об обязательном пенсионном страховании в Российской Федерации";
- ст.9; ст.14; ст.15 Федерального закона от 01.04.1996 №27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования";
- ст.9 Федерального закона от 30.04.2008 №56-ФЗ "О дополнительных страховых взносах на накопительную пенсию и государственной поддержке формирования пенсионных накоплений";
- ст.8- ст.14 Федерального закона от 28.12.2013 №400-ФЗ "О страховых пенсиях".

[21] См.:

- т. 95 Федерального закона от 29.12.2012 №273-ФЗ "Об образовании в Российской Федерации";
- ч.6 ст.16 Федерального закона от 12.06.2002 №67-ФЗ "Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации";
- ч.5 ст.8 Федерального закона от 18.07.2006 №109-ФЗ "О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации" и др.

[22] См.:

- ст.3.18 и ст. 9.9. ГОСТ Р ИСО 15489-1-2019. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы;

8.3.1. Уничтожение документов, содержащих конфиденциальную информацию, производится по акту экспертной комиссии, утвержденному министром, а так же может регламентироваться отдельными приказами Министерства в части не противоречащих настоящему Положению.

8.3.2. Отобранные к уничтожению документы измельчаются механическим способом до степени, исключающей возможность прочтения текста, или сжигается в печи до золы[22].

8.3.3. Конфиденциальная информация, хранящаяся на магнитных носителях, подлежит обязательному удалению путём полного форматирования носителя.

8.3.4. В целях гарантированного уничтожения файлов и затирания остаточной информации на магнитном носителе либо уничтожения носителей механическим способом ПДЭК может привлечь администратора безопасности информации, чтобы зафиксировать факт уничтожения.

8.3.5. 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 министром[23]. Результаты проведенных проверок рассматриваются на оперативных совещаниях при министре для предотвращения инцидентов с конфиденциальной информации в будущем.

9. Ответственность и полномочия персонала

9.1. Ответственность персонала

9.1.1 Ответственность за несоблюдение требований, установленных настоящим Положением, несут:

9.1.1.1 министр как первый руководитель данного органа государственной власти несет ответственность за организацию оборота в Министерстве информации ограниченного доступа и финансирование работ по защите конфиденциальной информации в соответствии с требованиями по безопасности информации[24];

9.1.1.2. заместитель министра, ответственный за организацию обработки персональных данных в Министерстве, несет ответственность за осуществление контроля организации допуска сотрудников Министерства и сотрудников иных органов и организаций к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности;

9.1.1.3. начальник отдела кадров Министерства отвечает за организацию допуска сотрудников Министерства и сотрудников иных органов и организаций к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности;

9.1.1.4. начальник общего отдела Министерства, отвечает за организацию конфиденциального делопроизводства в Министерстве;

9.1.1.5. администратор безопасности информации за осуществление защиты конфиденциальной информации в информационных системах;

9.1.1.6. системный администратор отвечает за поддержание установленного уровня защищенности информационных систем, обрабатывающих конфиденциальную информацию;

9.1.1.7. начальники управлений и отделов Министерства отвечают за контроль и организацию выполнения требований настоящего Положения во вверенных им подразделениях;

9.1.1.8. сотрудники Министерства 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.

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

9.1.3. 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.

9.2. Полномочия персонала

– ст.105 ГОСТ Р 7.0.8-2013. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения.

[23] 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, 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;

– п.5.1.4, п.7.3.4 ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности и Приложение А к указанному ГОСТ.

[24] В соответствии с:

– п.2.18 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;

– п.5.1 ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

Сотрудники Министерства имеют право выходить с предложениями к руководству Министерства по вопросам защиты конфиденциальной информации.