Утверждено

приказом Специального управления ФПС №5 МЧС России

от 09.04.2021 2021 №197

**ПОЛОЖЕНИЕ**

**об обработке персональных данных**

**в Специальном управлении ФПС №5 МЧС России**

**І. Общие положения**

1. Положение об обработке персональных данных в Специальном управлении ФПС №5 МЧС России[[1]](#footnote-1) разработано на основании Федерального закона Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 15 сентября 2008 г №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа МЧС России от 31.10.2019 №626 «Об обработке и обеспечении защиты персональных данных в Министерстве Российской Федерации по делам гражданской оборон, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий», ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности организации. Основные термины и определения».

2. Настоящее Положение является основным документом, определяющим политику Специального управления ФПС №5 МЧС России[[2]](#footnote-2) в отношении обработки персональных данных[[3]](#footnote-3), а также устанавливающим процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

3. В Положении используются следующие понятия и определения:

безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность;

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;

оператор - государственный орган, муниципальный орган, юридиче­ское или физическое лицо, организующие и (или) осуществляющие обработ­ку персональных данных, а также определяющие цели и содержание обра­ботки персональных данных;

обработка персональных данных - действия (операции) с персональ­ными данными, включая сбор, систематизацию, накопление, хранение, уточ­нение (обновление, изменение), использование, распространение (в том чис­ле передачу), обезличивание, блокирование, уничтожение персональных данных;

уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информаци­онной системе персональных данных или в результате которых уничтожают­ся материальные носители персональных данных;

уполномоченное лицо - лицо, которому оператор поручает обработку персональных данных;

несанкционированный доступ - дос­туп к информации или действия с информацией, осуществляемый с нарушением установленных прав и (или) правил доступа.

4. Ознакомление с настоящим Положением сотрудников (работников) Управления организуется начальником подразделения Управления при приеме на службу.

**ІІ. Организация работы с персональными данными**

1. Управление является оператором, осуществляющим обработку персональных данных, на основании приказа МЧС России от 31.10.2019 №626. Ответственный за организацию обработки персональных данных в Управлении назначается приказом начальника Управления. Задачи, функции и права ответственного по вопросам организации обработки персональных данных в Управлении отражаются в его должностном регламенте (должностной инструкции).

2. Обработка персональных данных поручается уполномоченным лицам путем издания приказа. Обязанности по обработке персональных данных сотрудников, уполномоченных на обработку персональных данных, отражаются в их должностных регламентах (должностных инструкциях). Уполномоченные лица допускаются к обработке персональных данных после ознакомления с положениями законодательства Российской Федерации и локальными актами МЧС России по вопросам обработки персональных данных, а также подписания обязательств о прекращении обработки персональных данных, ставших известными им в связи с исполнением должностных обязанностей, в случае расторжения контракта (трудового договора).

3. Перечень уполномоченных на обработку персональных данных может быть дополнен на основании рапорта начальника подразделения.

4. Категории субъектов персональных данных, порядок получения, перечень действий (операций), цели обработки и состав персональных данных определены приказом МЧС России от 31.10.2019 №626.

5. Согласие на обработку персональных данных и формы разъяснений субъектам персональных данных юридических последствий отказа предоставить свои персональные данные подшиваются в личные дела.

**ІІІ. Требования к защите персональных данных**

1. Размещение и оборудование помещений, в которых хранятся носители персональных данных, должны исключать возможность бесконтрольного проникновения в эти помещения посторонних лиц и гарантировать сохранность находящихся в них носителей персональных данных, а также отвечать правилам техники безопасности, санитарным нормам и требованиям пожарной безопасности. Входные двери помещений, в которых хранятся носители персональных данных, оборудуются замками, гарантирующими надежное закрытие помещений в нерабочее время, а также при выходе из него в рабочее время.

2. В помещения, в которых хранятся носители персональных данных, допускаются руководство Управления и подразделений Управления, а также должностные лица, имеющие прямое отношение к осуществлению обработки персональных данных. Список лиц, допущенных в помещение, разрабатывается руководителем подразделения, за которым закреплено помещение, утверждается ответственным за организацию обработки персональных данных. Доступ других лиц осуществляется только в сопровождении сотрудников (работников), ответственных за находящиеся в этих помещениях персональные данные.

3. Носители персональных данных должны храниться в шкафах. Допускается хранение носителей персональных данных на открытых стеллажах при условии размещения стеллажей способом, исключающим возможность несанкционированного доступа к ним.

4. Уборка и другие необходимые хозяйственные работы в помещениях, в которых хранятся носители персональных данных, производятся в присутствии лиц, отвечающих за находящиеся в этих помещениях персональные данные. При этом носители персональных данных должны располагаться таким образом, чтобы исключить возможность ознакомления с персональными данными посторонних лиц.

5. Рабочие места, в том числе автоматизированные, на которых обрабатываются персональные данные, должны быть размещены способом, исключающим несанкционированный доступ к персональным данным.

6. Хранение персональных данных с разными целями обработки персональных данных осуществляется на разных носителях.

7. Пересылка персональных данных по незащищенным каналам связи запрещена.

8. Персональные данные могут быть использованы уполномоченными лицами только для достижения целей, с которыми они получены.

9. Уполномоченные лица должны соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, соблюдать требования к защите обрабатываемых персональных данных, определенные настоящим Положением, а также иными нормативно-правовыми актами.

**ІV. Требования к защите персональных данных при их обработке в информационных системах**

1. Перечень информационных систем, в которых осуществляется обработка персональных данных, утверждается приказом.

2. Обработка персональных данных в информационных системах персональных данных осуществляется после определения уровня защищенности при соблюдении следующих правил разграничения доступа:

* доступ пользователей осуществляется по учетной записи, состоящей из имени пользователя и пароля;
* доступ и права для учетной записи настраиваются администратором безопасности;
* администратор безопасности организует регистрацию и учет всех действий, совершаемых в информационной системе персональных данных, и контролирует доступ пользователей к ресурсам информационной системы;
* соблюдаются требования к помещениям, в которых проводятся работы с персональными данными (хранятся материальные носители персональных данных).

3. Подключение к средствам информатизации, предназначенным для работы с информационной системой персональных данных, съемных машинных носителей информации возможно только после проверки администратором безопасности на предмет наличия вируса и несанкционированного вывода из информационной системы информации.

4. Машинные носители, используемые при обработке персональных данных в информационных системах, должны быть учтены в соответствующем журнале учета.

**V. Порядок уничтожения**

**персональных данных и их материальных носителей**

1. Уничтожение материальных носителей персональных данных осуществляется экспертной комиссией Управления, назначенной приказом начальника Управления.

2. Персональные данные подлежат уничтожению при достижении целей, с которыми они были получены, по истечении срока хранения и утрате практического значения. Срок хранения документов определяется в соответствии с «Перечнем документов, образующихся в деятельности органов управления, спасательных воинских формирований МЧС России, подразделений ФПС ГПС, Государственной инспекции по маломерным судам МЧС России, учреждений и организаций, находящихся в ведении МЧС России, с указанием сроков хранения». Исключение составляют черновики и проекты документов, которые уничтожаются исполнителем документов способом, исключающим возможность восстановить содержание персональных данных.

3. После выделения материальных носителей персональных данных с истекшими сроками хранения и проведения экспертизы ценности документов экспертная комиссия принимает решение об уничтожении с оформлением протокола.

4. Уничтожение отобранных материальных носителей персональных данных производится в возможно короткий срок, но не позднее 60 суток после утверждения акта, в безопасной зоне, которая исключает доступ посторонних лиц. Если подлежащие уничтожению документальные материалы вывозятся за пределы Управления, то они должны быть уничтожены в день вывоза.

5. Уничтожение материальных носителей персональных данных возможно путем измельчения при помощи шредера и (или) сжигания.

6. Перед уничтожением материальные носители персональных данных проверяются на предмет соответствия акту о выделении к уничтожению. После уничтожения члены комиссии заверяют факт уничтожения подписью в акте.

7. Утвержденный начальником Управления акт о выделении к уничтожению материальных носителей персональных данных является основанием для снятия материального носителя с учета.

**VІ. Организация контроля**

1. Организация контроля за соблюдением установленного порядка обращения с персональными данными в Управлении возлагается на заместителя начальника Управления.

2. Выполнение мероприятий, направленных на предотвращение и выявление нарушений законодательства Российской Федерации по вопросам защиты персональных данных, устранение последствий таких нарушений возлагается на комиссию по защите информации, не составляющей государственную тайну[[4]](#footnote-4).

3. Комиссия осуществляет свою деятельность на основании плана проверок условий обработки персональных данных.

**VІІ. Ответственность**

1. За нарушение требований к защите персональных данных предусмотрена дисциплинарная, гражданско-правовая, административная или уголовная ответственность в соответствии с действующим законодательством Российской Федерации.

2. Ответственность за обработку уполномоченными на обработку персональных данных и допуск к персональным данным в подразделениях Управления возлагается на руководителей подразделений.

1. далее - Положение [↑](#footnote-ref-1)
2. далее - Управление [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)
4. далее - Комиссия [↑](#footnote-ref-4)