МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ЧЕЧЕНСКОЙ РЕСПУБЛИКИ
Государственное бюджетное профессиональное образовательное учреждение
«Аргунский государственный механико-технологический техникум»

ПРИНЯТО
решением Педагогического
совета техникума
от «17» 01 2025 г.
Протокол № 3

УТВЕРЖДЕНО
Директор ГБПОУ «Аргунский
государственный механико-
технологический техникум»
М-Р.Р.Абдулхаджиев
от «20» 01 2025 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00F285FC4E76472A45363E964ABACABFF4
Владелец: Абдулхаджиев Магомед-Расул Русланович
Действителен: с 09.07.2024 до 02.10.2025

ПОЛОЖЕНИЕ 1
об обработке персональных данных в государственном бюджетном профессиональном образовательном учреждении «Аргунский государственный механико-технологический техникум»

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами

несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту 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.

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.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации,

возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе 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.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Учреждение – учреждения здравоохранения, социальной сферы, труда и занятости.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ –	Автоматизированное рабочее место
ИБ –	Информационная безопасность
ИС –	Информационная система
ИСПДн –	Информационная система персональных данных
ЛВС –	Локальная вычислительная сеть
НД –	Нормативный документ
НЖМД –	Накопитель на жестких магнитных дисках
НСД –	Несанкционированный доступ
ОИ –	Объект информатизации
ОС –	Операционная система
ПДн –	Персональные данные
ПО –	Программное обеспечение

ППО –	Прикладное программное обеспечение
ПЭВМ –	Персональная электронная вычислительная машина
САЗ –	Система антивирусной защиты
СВТ –	Средства вычислительной техники
СЗПДн –	Система защиты персональных данных
СКС –	Структурированная кабельная система
СОИБ –	Система обеспечения информационной безопасности
СТЗ –	Специальное техническое задание
ТЗ –	Техническое задание
ТС –	Технические средства
УФК –	Управление федерального казначейства по Чеченской Республике
УФНС –	Управление федеральной налоговой службы по Чеченской Республике
ФИО –	Фамилия имя отчество
ФСБ РФ –	Федеральная служба безопасности Российской Федерации
ФСТЭК РФ –	Федеральная служба по техническому и экспортному контролю Российской Федерации

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Цели и сфера действия

Положение об обработке персональных данных (далее – Положение) определяет требования к порядку обработки и защите (обеспечению безопасности) персональных данных обучающихся (субъектов ПДн) и сотрудников государственного бюджетного профессионального образовательного учреждения «Аргунский государственный механико-технологический техникум» (далее – техникум) с использованием средств автоматизации или без использования таких средств.

Целью настоящего Положения является соблюдение прав и свобод человека и гражданина при обработке его ПДн в информационных системах техникума, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Мероприятия по обеспечению безопасности ПДн являются составной частью деятельности техникума.

Действие Положения распространяется на все структурные подразделения техникума.

Настоящий документ является локальным нормативным актом техникума и вступает в силу с момента утверждения его директором техникума.

1.2. Законодательство Российской Федерации в области ПДн

Основными законодательными и нормативно-правовыми актами Российской Федерации в области персональных данных являются:

- Конституция Российской Федерации.

- Федеральный закон от 19.12.2005 №160-ФЗ «О ратификации конвенции совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

- Постановление Правительства Российской Федерации от 17.11.2007 №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

- Постановление Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

- Постановление Правительства Российской Федерации от 06.07.08 №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

- Приказ Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 №55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».

- Приказ Федеральной службы по техническому и экспортному контролю от 05.02.2010 № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.

- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/5-144

- Типовые требования 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 обработке в информационных системах персональных данных. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/6/6-622

1.3. Принципы обработки ПДн

Обработка ПДн осуществляется на основе принципов:

1) законности целей и способов обработки ПДн и добросовестности;

2) соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям техникума, как оператора ПДн;

3) соответствия объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;

4) достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;

5) недопустимости объединения созданных для несовместимых между собой целей баз данных ИСПДн.

1.4. Способы обработки ПДн

Техникум может осуществлять обработку ПДн с использованием средств автоматизации, а также без использования таких средств.

1.5. Условия обработки ПДн

При обработке персональных данных должны соблюдаться условия конфиденциальности ПДн. В соответствии с Указом Президента Российской Федерации от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера», персональные данные относятся к конфиденциальной информации. В техникуме документально оформляется перечень сведений конфиденциального характера.

Техникум и третьими лицами, получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных, за исключением следующих случаев:

1) в случае обезличивания ПДн;

2) в отношении общедоступных ПДн

1.6. Хранение и уничтожение ПДн

Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Для уничтожения ПДн, Приказом директора техникума назначается комиссия по уничтожению ПДн. Уничтожение ПДн оформляется актом.

Места хранения материальных носителей ПДн утверждаются Приказом директора техникума.

1.7. Взаимодействие с федеральными органами исполнительной власти

Взаимодействие с федеральными органами исполнительной власти по вопросам обработки и защиты ПДн субъектов, ПДн которых обрабатываются техникумом, осуществляется в рамках законодательства Российской Федерации.

СУБЪЕКТЫ И КАТЕГОРИИ ПДН

2.1. Субъекты ПДн

Техникумом (оператором персональных данных) осуществляется обработка ПДн следующих категорий субъектов ПДн:

1) обучающиеся – физические лица, которых связывают с технику договорными обязательствами отношения об оказании услуг;

2) сотрудники – физические лица, вступившие в трудовые отношения с работодателем;

2.2. Категории ПДн

В информационных системах техникума осуществляется обработка следующих категорий персональных данных:

- персональные данные, позволяющие идентифицировать субъекта ПДн;

- обезличенные ПДн.

МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН

3.1. Общие положения

Организация работ по обеспечению безопасности ПДн осуществляется руководством техникума.

Для разработки и осуществления мероприятий по обеспечению безопасности ПДн при их обработке в информационных системах техникума, приказом директора назначается ответственный за обеспечение безопасности ПДн (ответственный за информационную безопасности и обработку персональных данных).

Ответственный за информационную безопасности и обработку персональных данных).

безопасности ИСПДн в своей деятельности руководствуется «Положением о защите персональных данных».

Лица, доступ которых к ПДн, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПДн на основании утвержденного списка.

3.2. Мероприятия по обеспечению безопасности ПДн при автоматизированной обработке

3.2.1. Система защиты ПДн.

Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты ПДн, включающей организационные меры и средства защиты информации (далее – СЗИ) (в том числе криптографические, средства предотвращения НСД, утечки информации по техническим каналам, программно-технических воздействий на ТС обработки ПДн), а также используемые в информационной системе информационные технологии.

При обработке ПДн в техникуме должно быть обеспечено:

- Проведение мероприятий, направленных на предотвращение НСД к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

- Своевременное обнаружение фактов НСД к ПДн;

- Недопущение воздействия на ТС автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

- Возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;

- Постоянный контроль над обеспечением уровня защищенности ПДн.

3.2.2. Перечень мероприятий по обеспечению безопасности ПДн.

Мероприятия по обеспечению безопасности ПДн при их обработке в информационных системах включают в себя:

- Определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;

- Разработку на основе модели угроз СЗПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса информационных систем;

- Проверку готовности СЗИ к использованию с составлением заключений о возможности их эксплуатации;

- Установку и ввод в эксплуатацию СЗИ в соответствии с эксплуатационной и технической документацией;

- Обучение лиц, использующих СЗИ, применяемые в ИСПДн, правилам работы с ними;

- Учет применяемых СЗИ, эксплуатационной и технической документации к ним, носителей ПДн.;

- Учет лиц, допущенных к работе с ПДн в информационной системе;

- Контроль над соблюдением условий использования СЗИ, предусмотренных эксплуатационной и технической документацией;

- Разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования СЗИ, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- Описание системы защиты ПДн.

3.2.3. Классификация ИСПДн.

ИСПДн техникума подлежат обязательной классификации.

Для проведения классификации ИСПДн техникума приказом директора назначается комиссия.

Результаты классификации оформляются соответствующим актом.

3.2.4. Помещения, в которых ведется обработка ПДн.

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с ПДн, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей ПДн и СЗИ, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Порядок и правила доступа в помещения техникума регламентируются «Списком лиц, имеющим допуск в помещения ИСПДн».

3.3. Мероприятия по обеспечению безопасности ПДн при их обработке без использования средств автоматизации

Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн, либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

Лица, осуществляющие обработку ПДн без использования средств автоматизации, должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки.

3.4. Контроль и надзор за выполнением требований настоящего Положения

Контроль и надзор за выполнением требований настоящего Положения заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Он может проводиться ответственным за обеспечение безопасности ПДн, или на договорной основе сторонними организациями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.

4. Ответственность за нарушение требований настоящего положения

Лица, виновные в нарушении требований настоящего Положения, несут гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.

5. Персональные данные сотрудников техникума

Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

6.1. Цели обработки персональных данных

Обработка ПДн работников техникума осуществляется с целью обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

6.2. Перечень обрабатываемых персональных данных

Состав персональных данных работников:

- Фамилия, имя, отчество;

- Место, год и дата рождения;

- Адрес по прописке;

- Паспортные данные (серия, номер паспорта, кем и когда выдан);

- Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающих образование: наименование, номер, дата выдачи, специальность);

- Информация о трудовой деятельности до приема на работу;

- Информация о трудовом стаже (место работы, должность, период работы);

- Адрес проживания (реальный);

- Телефонный номер (домашний, рабочий, мобильный);

- Семейное положение и состав семьи (муж/жена, дети);

- Занимаемая должность;

- Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);

- ИНН;

- Страховое свидетельство государственного пенсионного фонда.

Запрещается требовать от лица, поступающего на работу, документы помимо предусмотренных Трудовым кодексом, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

6.3. Сроки хранения персональных данных

Сроки хранения документов устанавливаются согласно перечня типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения, утвержденного Руководителем Федеральной архивной службы России 06.10.2000.