

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ
ПРЕДПРИЯТИЕ «13 СУДОРЕМОНТНЫЙ ЗАВОД ЧЕРНОМОРСКОГО ФЛОТА»
МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ**



СТАНДАРТ ПРЕДПРИЯТИЯ

Система менеджмента качества

**ПОЛИТИКА
В ОБЛАСТИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

П-СП/СРиИБ-08

Редакция I - 2016

Севастополь

2016 г.

ПРЕДИСЛОВИЕ

1. Разработан и внесен ФГУП «13 судоремонтный завод Черноморского флота» Министерства обороны Российской Федерации.
2. Введен в действие приказом начальника ФГУП «13 СРЗ ЧФ» Минобороны России № 694 от «19» апреля 2016г.
3. Введен в действие впервые.
4. Периодическая проверка производится разработчиком с интервалом, не превышающим 12 месяцев.
5. Изменения разрабатываются и вносятся в настоящий стандарт по результатам его применения на ФГУП «13 СРЗ ЧФ» Минобороны России или при изменении требований нормативно - правовых актов, на основании которых разработан настоящий стандарт.

СОДЕРЖАНИЕ

1	Область применения	5
2	Нормативные ссылки	5
3	Термины, определения, сокращения	6
4	Общие положения	9
5	Правовые основания обработки персональных данных	10
6	Принципы и цели обработки персональных данных	11
7	Категории и перечень персональных данных, обрабатываемых на предприятии	13
8	Перечень субъектов, персональные данные которых обрабатываются на предприятии	13
9	Функции предприятия при осуществлении обработки персональных данных	14
10	Условия обработки персональных данных на предприятии	14
11	Перечень действий с персональными данными и способы их обработки	15
12	Меры, принимаемые предприятием для обеспечения выполнения обязанностей оператора при обработке персональных данных	16
13	Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов предприятия в области персональных данных	17
14	Конфиденциальность персональных данных	18
15	Меры по обеспечению безопасности персональных данных при их обработке	19
16	Права субъектов персональных данных	20
17	Контактная информация	22
18	Заключительные положения	22
19	Лист учета изменений	24
20	Лист периодических проверок	25
21	Лист ознакомления персонала	26

УТВЕРЖДАЮ
НАЧАЛЬНИК ФГУП «13 СРЗ ЧФ»
МИНОБОРОНЫ РОССИИ
капитан 2 ранга

Ю. Беспалов
« 18 » 04 2016 г.

П – СП/СРиИБ- 08

СТАНДАРТ ПРЕДПРИЯТИЯ

Система менеджмента качества

ПОЛИТИКА в области обработки и защиты персональных данных

Дата введения – 19 января 2016 г.

Рассмотрено и согласовано на заседании комиссии по персональным данным.
Протокол от «14» января 2016г. № 4.

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

- 1.1. Настоящая Политика устанавливает общие требования к организации обработки и защиты персональных данных на Предприятии.
- 1.2. Настоящая Политика обязательна для соблюдения и подлежит доведению до всех сотрудников Предприятия.
- 1.3. Контроль за соблюдением Политики осуществляет начальник ФГУП «13 СРЗ ЧФ» Минобороны России.

2. НОРМАТИВНЫЕ ССЫЛКИ

Политика разработана в соответствии с требованиями:

- Конституции РФ;
- Трудового кодекса РФ от 30.12.2001г. № 197 - ФЗ;
- Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных»;

- Указа Президента РФ от 06.03.1997г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Постановления Правительства РФ от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказа Минкультуры России от 25.08.2010г. № 558 «Об утверждении перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций с указанием сроков хранения»;
- ГОСТ Р ИСО/МЭК 27001 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
- ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»;
- ГОСТ Р 6.30-2003 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов»;
- Положения о системе менеджмента информационной безопасности ФГУП «13 СРЗ ЧФ» Минобороны России (приказ от 14.02.2014г. № 171).

3. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ

3.1. В настоящем документе используются следующие термины и их определения:

Блокирование персональных данных - временное прекращение обработки персональных данных работников (за исключением случаев, если обработка необходима для уточнения персональных данных);

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

Защита персональных данных – комплекс правовых, административных, технических и иных мер по предотвращению (пресечению) несанкционированного доступа к персональным данным либо их несанкционированного уничтожения, изменения, блокирования, копирования, предоставления или распространения.

Информация - сведения (сообщения, данные) независимо от формы их представления;

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных с использованием или без использования средств автоматизации;

Использование персональных данных - это действия 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;

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

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному работнику;

Обработка персональных данных работника - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Общедоступные источники персональных данных - минимальные сведения, составляющие круг ежедневного социального общения работника (имя, фамилия, отчество и пол, возраст, образование, адрес места жительства, номер телефона, сведения о профессии, ученых степенях и званиях) и которые он готов сообщить определенному кругу лиц и организаций;

Ограниченно обрабатываемые персональные данные - это различные виды персональных данных, в том числе и данные регистрационных номеров документов, сообщаемые Работником (с его согласия) Работодателю с целью совершения каких-либо действий или получения каких-либо услуг, а также информация о персональных данных работника содержащаяся в документальных материалах ООТЗ, канцелярии, секретного отделения, бухгалтерии, бюро пропусков;

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), и необходимая Работодателю в связи с трудовыми отношениями.

Под информацией о работнике понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

Передача персональных данных - действия оператора по

распространению, предоставлению, доступу к персональным данным;

Персональная ответственность – одно из главных требований к организации системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных работников определенному лицу или определенному кругу лиц;

Работник - физическое лицо, заключившее трудовой договор с Предприятием;

Распространение персональных данных - действия, направленные на раскрытие персональных данных работников неопределенному кругу лиц, в том числе обнародование в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Соискатель – физическое лицо, претендующее на заключение трудового договора с Предприятием;

Неавтоматизированная обработка персональных данных – действия по использованию, уточнению, распространению, уничтожению персональных данных в отношении каждого из субъектов персональных данных, содержащихся в информационной системе персональных данных, осуществленные при непосредственном участии человека. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее;

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

Угроза или опасность утраты персональных данных – единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию;

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных работников и (или) в результате которых уничтожаются материальные носители персональных данных работников;

3.2. В настоящем документе используются следующие сокращения:

Предприятие – ФГУП «13 СРЗ ЧФ» Минобороны России;

Политика - «Политика в области обработки и защиты персональных данных»;

ТК РФ – Трудовой кодекс Российской Федерации;

КоАП РФ – кодекс об административных правонарушениях;
ПЭВМ – персональная электронно-вычислительная машина;
ИСПДн – информационная система персональных данных.

4. ОБЩИЕ ПОЛОЖЕНИЯ

4.1. В целях поддержания деловой репутации и гарантирования выполнения норм федерального законодательства в полном объеме ФГУП «13 СРЗ ЧФ» Минобороны России (далее – Оператор) считает важнейшими своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение безопасности процессов их обработки.

4.2. «Политика в области обработки и защиты персональных данных (далее – Политика) является локальным нормативным актом ФГУП «13 СРЗ ЧФ» Минобороны России (далее - Предприятие),

4.3. Положения Политики служат основой для разработки локальных нормативных актов Предприятия, регламентирующих вопросы обработки и защиты персональных данных работников и других субъектов персональных данных.

4.4. Действующая редакция хранится в месте нахождения Оператора: Российская Федерация, город Севастополь, Нахимовский район, Килен-балка.

Электронная версия Политики размещена на официальном сайте Предприятия по адресу: 13srz.ru

4.5. Настоящая Политика:

- разработана в целях обеспечения реализации требований законодательства РФ в области обработки и защиты персональных данных субъектов персональных данных.

- определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов обрабатываемых на Предприятии персональных данных, функции Предприятия при обработке персональных данных, права субъектов персональных данных, а также реализуемые на Предприятии требования к защите персональных данных.

- является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке персональных данных.

4.6. Настоящая Политика вступает в силу с момента ее утверждения руководителем Предприятия и действует до введения новой Политики.

4.7. Все работники Предприятия должны быть ознакомлены под роспись с данной Политикой.

4.8. Внесение изменений в действующую Политику производится на основании приказа руководителя Предприятия.

5. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Политика в области обработки и защиты персональных данных определяется в соответствии со следующими нормативными правовыми актами РФ:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 19.12.2005 г. №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»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 29.11.2010 N 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Указ Президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
- Приказ ФСТЭК России от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»
- Приказ Министерства связи и массовых коммуникаций Российской Федерации от 14.11.2011 № 312 «Об утверждении Административного регламента исполнения федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства российской федерации в области персональных данных»;
- иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.

5.2. В целях реализации положений Политики на Предприятии разрабатываются соответствующие локальные нормативные акты и иные документы, в том числе:

- Положение о порядке обработки и защиты персональных данных;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные;
- Правила обработки персональных данных;
- Перечень обрабатываемых персональных данных;
- Перечень информационных систем персональных данных
- иные локальные нормативные акты и документы, регламентирующие на Предприятии вопросы обработки и защиты персональных данных.

6. ПРИНЦИПЫ И ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. ФГУП «13 СРЗ ЧФ» Минобороны России, являясь оператором персональных данных, осуществляет обработку персональных данных работников Предприятия и других субъектов персональных данных, не состоящих с Предприятием в трудовых отношениях.

6.2. Обработка персональных данных на Предприятии осуществляется с учетом необходимости обеспечения защиты прав и свобод работников Предприятия и других субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих **принципов**:

- обработка персональных данных осуществляется на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Предприятием принимаются необходимые меры либо обеспечивается их принятие по удалению или уточнению неполных или неточных персональных данных;

- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.7. Персональные данные обрабатываются на Предприятии **в целях:**

- обеспечения соблюдения Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов Предприятия;
- осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на предприятие, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд Российской Федерации, в Фонд социального страхования Российской Федерации, в Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы;
- регулирования трудовых отношений с работниками Предприятия (содействие в трудоустройстве, обучение и продвижение по службе, обеспечение личной безопасности, контроль количества и качества выполняемой работы, обеспечение сохранности имущества);
- ведения кадровой работы, в том числе при формировании кадрового резерва;
- защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;
- подготовки, заключения, исполнения и прекращения договоров с контрагентами;
- обеспечения пропускного и внутриобъектового режимов на объектах Предприятия;
- формирования справочных материалов для внутреннего информационного обеспечения деятельности Предприятия;
- исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- осуществления прав и законных интересов Предприятия в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Предприятия, или третьих лиц либо достижения общественно значимых целей;
- в иных законных целях.

7. КАТЕГОРИИ И ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ НА ПРЕДПРИЯТИИ

7.1. Оператор осуществляет обработку:

- общедоступных персональных данных;
- биометрических персональных данных (сведения: фотография и видеозапись, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность, и используемые для обеспечения однократного или многократного прохода на охраняемую территорию и установления личности субъекта).

7.2. Оператор не выполняет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

7.3. Оператор не производит трансграничную (на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.

7.4. Оператором созданы общедоступные источники персональных данных (справочники, адресные книги). Персональные данные, сообщаемые субъектом (фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и др.), включаются в такие источники только с письменного согласия субъекта персональных данных.

7.5. Перечень персональных данных, обрабатываемых на Предприятии, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами Предприятия с учетом целей обработки персональных данных, указанных в разделе 6 Политики.

Перечень персональных данных, подлежащих обработке, утверждается приказом начальника завода./

7.6. Сроки обработки персональных данных (хранения):

- сотрудников (работников) – 75 лет;
- членов семей сотрудников (работников) – в соответствии с действующим законодательством, но не менее 5 лет после проведения ревизии или проверки контролирующих органов;
- кандидатов на должность – 1 год;
- контрагентов и их представителей – 5 лет после проведения ревизии или проверки контролирующих органов.

8. ПЕРЕЧЕНЬ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ НА ПРЕДПРИЯТИИ

8.1. На Предприятии обрабатываются персональные данные следующих категорий субъектов:

- работников структурных подразделений предприятия;

- других субъектов персональных данных (для обеспечения реализации целей обработки, указанных в разделе 6 Политики).

9. ФУНКЦИИ ПРЕДПРИЯТИЯ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Предприятие при осуществлении обработки персональных данных:

- принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов Предприятия в области персональных данных;
- принимает правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;
- назначает лицо, ответственное за организацию обработки персональных данных на Предприятии;
- издает локальные нормативные акты, определяющие политику и вопросы обработки и защиты персональных данных на Предприятии;
- осуществляет ознакомление работников Предприятия непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локальных нормативных актов Предприятия в области персональных данных, в том числе требованиями к защите персональных данных, и обучение указанных работников;
- публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике;
- сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации;
- прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации в области персональных данных;
- совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных.

10. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ

10.1. Обработка персональных данных на Предприятии осуществляется с

согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных.

10.2. Предприятие без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

10.3. Предприятие вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, на основании заключаемого с этим лицом договора.

Договор должен содержать:

- перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных,
- цели обработки,
- обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке,
- требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

10.4. В целях внутреннего информационного обеспечения Предприятие может создавать внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться:

- его фамилия, имя, отчество,
- год и место рождения,
- место работы, должность,
- адрес,
- абонентский номер,
- адрес электронной почты,
- иные персональные данные, сообщаемые субъектом персональных данных.

10.5. Доступ к обрабатываемым на Предприятии персональным данным разрешается только работникам Предприятия, занимающим должности, включенные в перечень должностей структурных подразделений Предприятия, при замещении которых осуществляется обработка персональных данных.

11. ПЕРЕЧЕНЬ ДЕЙСТВИЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ И СПОСОБЫ ИХ ОБРАБОТКИ

11.1. На Предприятии операторами используются следующие действия по обработке персональных данных:

сбор, запись, систематизация, накопление, хранение, уточнение, извлечение, использование, передача, обезличивание, блокирование, удаление, уничтожение.

11.2. Обработка персональных данных на предприятии осуществляется следующими способами:

- неавтоматизированная обработка персональных данных;
- неавтоматизированная обработка биометрических персональных данных (фотографическое изображение субъекта персональных данных).
- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям;
- смешанная обработка персональных данных с применением ЭВМ.

11.3. Перечень объектов информатизации (информационных систем) персональных данных Предприятия утверждается начальником Предприятия. Информационные системы персональных данных классифицируются в зависимости от категорий, обрабатываемых в них персональных данных.

12. МЕРЫ, ПРИНИМАЕМЫЕ ПРЕДПРИЯТИЕМ ДЛЯ ОБЕСПЕЧЕНИЯ ВЫПОЛНЕНИЯ ОБЯЗАННОСТЕЙ ОПЕРАТОРА ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

12.1. Меры, необходимые и достаточные для обеспечения выполнения Предприятием обязанностей оператора, предусмотренных законодательством Российской Федерации в области персональных данных, включают:

- назначение лица, ответственного за организацию обработки персональных данных на Предприятии;
- принятие локальных нормативных актов и иных документов в области обработки и защиты персональных данных;
- организацию обучения и проведение методической работы с работниками структурных подразделений Предприятия, занимающими должности, включенные в перечень должностей структурных подразделений Предприятия, при замещении которых осуществляется обработка персональных данных;
- получение согласий субъектов персональных данных на обработку их персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации;
- обособление персональных данных, обрабатываемых без использования средств автоматизации, от иной информации, в частности путем их фиксации на отдельных материальных носителях персональных данных, в специальных разделах;
- обеспечение раздельного хранения персональных данных и их материальных носителей, обработка которых осуществляется в разных целях и которые содержат разные категории персональных данных;
- установление запрета на передачу персональных данных по открытым каналам связи, вычислительным сетям вне пределов контролируемой зоны, и сетям Интернет без применения установленных мер по обеспечению

- безопасности персональных данных (за исключением общедоступных и (или) обезличенных персональных данных);
- хранение материальных носителей персональных данных с соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним;
 - осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам Предприятия;
 - иные меры, предусмотренные законодательством Российской Федерации в области персональных данных.

12.2. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются в соответствии с локальными нормативными актами Предприятия, регламентирующими вопросы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Предприятия.

13. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ И ЛОКАЛЬНЫХ НОРМАТИВНЫХ АКТОВ ПРЕДПРИЯТИЯ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

13.1. Контроль за соблюдением структурными подразделениями Предприятия законодательства Российской Федерации и локальных нормативных актов Предприятия в области персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки:

- соответствия обработки персональных данных в структурных подразделениях Предприятия законодательству Российской Федерации и локальным нормативным актам Предприятия в области обработки и защиты персональных данных,

- принятых мер, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в области обработки и защиты персональных данных.

13.2. Внутренний контроль за соблюдением структурными подразделениями Предприятия законодательства Российской Федерации и локальных нормативных актов Предприятия в области персональных данных, в том числе требований к защите персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных на Предприятии.

13.3. Внутренний контроль соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных,

настоящей Политике, локальным нормативным актам Предприятия осуществляет служба режима и информационной безопасности Предприятия.

13.4. Персональная ответственность за соблюдение требований законодательства Российской Федерации и локальных нормативных актов Предприятия в области персональных данных в структурных подразделениях Предприятия, а также за обеспечение конфиденциальности и безопасности персональных данных в указанных подразделениях Предприятия возлагается на их руководителей.

14. КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

14.1. Информация, относящаяся к персональным данным, является конфиденциальной информацией и охраняется законом.

Все меры конфиденциальности при обработке и защите персональных данных распространяются на все материальные носители информации (бумажные, электронные).

14.2. Оператор несет ответственность за обеспечение конфиденциальности предоставленных сведений с момента их получения.

Оператор не несет ответственности за конфиденциальность персональных данных при получении их на официальные электронные адреса Оператора по открытым каналам связи.

14.3. Работники предприятия, ответственные за обработку персональных данных, а также сотрудники предприятия, владеющие персональными данными в силу своих должностных обязанностей:

- подписывают обязательство о неразглашении информации, содержащей персональных данных;
- предупреждаются о возможной дисциплинарной, административной, гражданско-правовой и уголовной ответственности за нарушения норм и требований действующего законодательства Российской Федерации в области обработки и защиты персональных данных.

14.4. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Оператор в ходе своей деятельности предоставляет персональные данные следующим организациям:

- Федеральной налоговой службе;
- Пенсионному фонду России;
- негосударственным пенсионным фондам;
- страховым компаниям;
- кредитным организациям;
- лицензирующим и/или контролирующим органам государственной власти и местного самоуправления.

14.5. По мотивированному запросу исключительно для выполнения возложенных законодательством функций и полномочий персональные данные

субъекта персональных без его согласия могут быть переданы:

- в судебные органы в связи с осуществлением правосудия;
- в органы федеральной службы безопасности;
- в органы прокуратуры;
- в органы полиции;
- в иные органы и организации в случаях, установленных нормативными правовыми актами, обязательными для исполнения.

15. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

15.1. Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них.

15.2. Структура, состав и основные функции системы защиты персональных данных определяются исходя из класса ИСПДн.

Система защиты персональных данных включает организационные меры и технические средства защиты информации, а также используемые в информационной системе информационные технологии.

15.3. Технические и программные средства, используемые для обработки персональных данных в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

15.4. Обеспечение безопасности персональных данных при их обработке достигается:

15.4.1. Разработкой локальных нормативно-правовых актов в отношении обработки и защиты персональных данных;

15.4.2. Назначением ответственных за организацию обработки и защиты персональных данных.

15.4.3. Осуществлением внутреннего контроля и/или аудита соответствия обработки и защиты персональных данных требованиям нормативно-правовых актов.

15.4.4. Ознакомлением работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и (или) обучением указанных сотрудников.

15.4.5. Определением угроз безопасности персональных данных при их

обработке в информационных системах персональных данных, и разработкой мер и мероприятий по защите персональных данных.

15.4.6. Применением организационных, правовых и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

15.4.7. Учетом машинных носителей персональных данных.

15.4.8. Выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.

15.4.9. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

15.4.10. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных.

15.4.11. Установлением индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их трудовыми обязанностями;

15.4.12. Применением сертифицированных средств защиты информации, антивирусного программного обеспечения, программных средств защиты информации от несанкционированного доступа.

15.4.13. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

15.4.14. Соблюдением условий, обеспечивающих сохранность персональных данных и исключают несанкционированный к ним доступ;

15.5. Обязанности должностных лиц, осуществляющих обработку и защиту ПДн, а также их ответственность, определяются в «Положении о порядке обработки и защиты персональных данных»

16. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

16.1. Субъект персональных данных имеет право на получение полной информации об обработке его персональных данных Оператором.

16.2. Субъект персональных данных вправе требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

16.3. Субъект персональных данных имеет право на доступ к своим персональным данным, включая право на получение копии любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных федеральными законами.

16.4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе в следующих случаях:

16.4.1. Если обработка персональных данных, включая те, что получены в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, выполняется в целях укрепления обороны страны, обеспечения безопасности государства и охраны правопорядка.

16.4.2. При условии, что обработка персональных данных производится органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, когда допускается ознакомление подозреваемого или обвиняемого с такими персональными данными.

16.4.3. Если обработка персональных данных выполняется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

16.4.4. Когда доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

16.4.5. Если обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

16.5. Для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться к Оператору.

Оператор обязан рассмотреть любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследовать факты нарушений и принять все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

16.6. Субъект персональных данных вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите прав субъектов персональных данных или в суд.

16.7. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

16.8. Субъект персональных данных имеет право на отзыв согласия на обработку персональных данных, а также осуществление иных прав, предусмотренных законодательством Российской Федерации.

17. КОНТАКТНАЯ ИНФОРМАЦИЯ

17.1. Наименование оператора: ФГУП «13 СРЗ ЧФ» Минобороны России
ИНН: 9203501030

Место нахождения Предприятия:

Российская Федерация, город Севастополь, Нахимовский район, Килен-балка.
тел/факс (0692) 40-13-52,
e-mail: sev_13srz@mail.ru

Почтовый адрес: 299004, Россия, город Севастополь, Килен-балка, ФГУП «13 СРЗ ЧФ» Минобороны России.

17.2. Ответственным за организацию обработки и обеспечения безопасности персональных данных на ФГУП «13 СРЗ ЧФ» Минобороны России назначен начальник службы режима и информационной безопасности,

тел.: (0692) 40 13 29,
e-mail: riib@13srz.ru

17.3. Уполномоченным органом по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Управление по защите прав субъектов персональных данных.

Управление Роскомнадзора по Республике Крым и г. Севастополь:

Адрес: 295050, ул. Вилар, д.4, г. Симферополь, Республика Крым

Телефон: 8 3652 669-293
8 978 990-33-22

e-mail: rsockanc82@rkn.gov.ru

Сайт 82.rkn.gov.ru

18. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

18.1. Настоящая Политика разрабатывается службой режима и информационной безопасности и утверждается начальником ФГУП «13 СРЗ ЧФ» Минобороны России.

18.2. Срок действия настоящей Политики – один год с момента утверждения. По истечении срока действия (при необходимости – ранее) Политика подлежит пересмотру. Внесение изменений в Политику производит служба режима и информационной безопасности. Пересмотренная Политика утверждается начальником ФГУП «13 СРЗ ЧФ» Минобороны России.

18.3. Настоящая Политика обязательна для соблюдения и подлежит доведению до всех работников ФГУП «13 СРЗ ЧФ» Минобороны России.

Контроль за соблюдением Политики осуществляет служба режима и информационной безопасности.

Разработал:

Начальник службы режима и информационной безопасности

О.Сечкин

Согласовано:

Помощник начальника завода по безопасности

И. Качковенко

Юрисконсульт 1 категории

Т. Першина

О внесении изменений

В печатном варианте локального акта «Политика в области обработки и защиты персональных данных» на основании приказа от 31.05.2016г. № 968 «О внесении изменений в локальные акты ФГУП «13 СРЗ ЧФ» Минобороны России в области персональных данных» внесены следующие изменения:

- в п. 7.1. (*стр. 13*) добавлена фраза: «- специальных категорий персональных данных (состояние здоровья работников предприятия)»

- из п. 7.2. (*стр. 13*) исключена фраза: « ...состояния здоровья...»

В листе учета изменений «Политики в области обработки и защиты персональных данных» сделаны соответствующие отметки.