УТВЕРЖДАЮ

Генеральный директор

АО «ННПО имени М.В.Фрунзе»

Н.А.Воронов

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

Акционерного общества «Нижегородское научно – производственное объединение имени М.В.Фрунзе»

(далее АО «ННПО имени М.В.Фрунзе»)

г. Нижний Новгород

2017 год

1. Общие положения

1.1 Настоящее Положение разработано на основании Конституции РФ, Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, а также Федеральных законов: «Об информации, информатизации и защите информации» и «О персональных данных».

1.2 Настоящее Положение определяет комплекс мер, направленных на обеспечение защиты персональных данных работников АО «ННПО имени М.В.Фрунзе» от несанкционированного доступа к ним, неправомерного их использования или утраты.

1.3 Основные цели и задачи, принципы обеспечения безопасности персональных данных, а так же общую стратегию построения системы защиты персональных данных (СЗПДн) предприятия определены в Концепции информационной безопасности, утвержденной в установленном порядке приказом генерального директора, и являющейся неотъемлемым приложением к настоящему Положению.

1.4 Категории конкретных мероприятий по обеспечению безопасности ПДн определены в Политике информационной безопасности, утвержденной в установленном порядке приказом генерального директора, и являющейся неотъемлемым приложением к настоящему Положению.

1.5 Персональные данные относятся к категории конфиденциальной информации.

1.6 Настоящие Положение утверждается и вводится в действие приказом генерального директора и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным работников предприятия.

1.7 При заключении трудового договора с вновь принимаемым на завод работником, сотрудник отдела по работе с персоналом обязан ознакомить последнего с настоящим положением под роспись.

2. Понятие и состав персональных данных

2.1 Персональные данные работника – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обязательствах жизни работника, позволяющие идентифицировать его личность.

2.2 Состав персональных данных в АО «ННПО имени М.В.Фрунзе» определен в Перечне персональных данных в АО «ННПО имени М.В.Фрунзе», утвержденном приказом генерального директора предприятия, являющемся неотъемлемым приложением к настоящему Положению.

3. Обработка персональных данных

3.1 Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение,

уточнение (обновление, изменение), использование, распространение (в том числе передача) обезличивание, блокирование, уничтожение персональных данных.

3.2 К обработке персональных данных имеют доступ сотрудники предприятия, указанные в приказе о назначении ответственных лиц за обработку персональных данных и положении о разграничении прав доступа к обрабатываемым персональным данным. Обработка персональных данных на предприятии производится на основании письменного согласия по форме приложения к настоящему Положению, которое оформляется при подборе кандидатов на вакантные должности или при оформлении на работу.

3.3 В целях обеспечения прав и свобод человека и гражданина, работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

3.3.1 Обработка персональных данных работника может осуществляться исключительно в целях 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 и других действий, связанных с трудовыми отношениями.

3.3.2 При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.

3.3.3 Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их из иных источников, а так же от сотрудников предприятия.

3.3.4 Персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Сотрудники предприятия должны сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.3.5 Предприятие не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны работодателем только с его письменного согласия.

3.3.6 Предприятие не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.4 Использование персональных данных возможно только в соответствии с целями, определившими их получение.

Персональные данные не могут быть использованы предприятием в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав

граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено.

3.5 Передача персональных данных работника возможна только с согласия работника, выраженного в письменной форме, или в случаях, прямо предусмотренных законодательством.

3.5.1 При передаче персональных данных работника предприятие обязано соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральными законами;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по организации, при этом, указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- передавать персональные данные работника представителям работника в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми данными работника, которые необходимы для выполнения указанными представителями их функций.

3.5.2 Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

3.5.3 При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы предприятия, предприятие не должно сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральными законами;

3.6 Действие настоящего положения при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации;

3.7 Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

3.8 Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

3.9 При принятии решений, затрагивающих интересы работника, предприятие не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Предприятие учитывает личные качества работника, его добросовестный и эффективный труд.

4. Доступ к персональным данным

4.1 Внутренний доступ (доступ внутри предприятия).

4.1.1 Доступ к персональным данным имеют сотрудники предприятия, указные в приказе о назначении ответственных лиц за обработку персональных данных и в положении о разграничении прав доступа к обрабатываемым персональным данным.

4.1.2 Лица, указанные в п. 4.1.1 за исключением самого работника, при обработке, исполнении, передаче, хранении персональных данных обязаны выполнять требования, названные в разделе 3 настоящего Положения.

4.1.3 Доступ к персональным данным работников генерального директора и заместителя генерального директора по безопасности должен быть обеспечен начальником подразделения, в котором осуществляется обработка соответствующих персональных данных в сроки, указанные этим руководителем.

4.1.4 Руководители структурных подразделений и другие сотрудники предприятия при выполнении служебных обязанностей имеют право на доступ к персональным данным работников при наличии разрешающей визы начальника подразделения, в котором осуществляется обработка соответствующих персональных данных, на служебной записке, содержащей сведения о конкретном объеме персональных данных, к которым необходим доступ, причинах необходимости доступа к ним, а также форме доступа (знакомство с соответствующими документами с оформлением выписок, оформление копий документов и др.).

4.1.5 При обращении либо при получении запроса от работника или его законного представителя сотрудники, имеющие доступ к обработке персональных данных работника, обязаны:

- сообщать работнику или его законному представителю информацию о наличии персональных данных, относящихся к нему, а также предоставить возможность ознакомления с ними при обращении работника или его законного представителя в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

- в случае отказа в предоставлении работнику или его законному представителю персональных данных при обращении работника, либо при получении им запроса об информации, дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 5 статьи 14 Федерального закона «О персональных данных» или иного Федерального закона, в срок, не превышающий семи рабочих дней со дня обращения работника или его законного представителя либо с даты получения запроса работника или его законного представителя;

- безвозмездно предоставлять работнику или его законному представителю возможность ознакомления с персональными данными, а также внести в них необходимые изменения;

- уничтожить или блокировать соответствующие персональные данные по предоставлении работником или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к работнику и обработку которых осуществляет сотрудник, имеющий доступ к обработке персональных данных работника, являются неполными, устаревшими, не достоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах сотрудник, имеющий доступ к обработке персональных данных работника, обязать уведомить работника или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы;

- по письменному заявлению работника не позднее трех дней со дня подачи этого заявления выдавать последнему копии документов, связанные с работой (копии приказа о приеме на работу, приказов о переводе на другую работу, приказа об увольнении с работы, выписки из трудовой книжки, справки о заработной плате, периоде работы у данного работодателя и другое). Копии документов, связанные с работой должны быть заверены надлежащим образом и предоставляться работнику безвозмездно;

- сообщать в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа в течении семи рабочих дней с даты получения такого запроса.

4.2 Внешний доступ.

4.2.1 К числу массовых потребителей персональных данных вне предприятия относятся государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военные комиссаритаты;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

4.2.2 Надзорно – контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.2.3 Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

4.2.4 Другим организациям сведения о работающем или уже уволенном сотруднике могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

4.2.5 Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника или на основании вступившего в законную силу решения суда.

5. Угроза безопасности персональных данных

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

5.2 Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

5.3 Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности предприятия.

5.4 Защита персональных данных работника от неправомерного их использования или утраты обеспечивается предприятием за счет его собственных средств и в порядке, установленным федеральным законом.

5.5 «Внутренняя защита».

5.5.1 Для обеспечении внутренней защиты персональных данных работников, предприятие обязуется соблюдать следующие меры:

- ограничить и регламентировать состав работников, функциональные обязанности которых требуют конфиденциальных знаний;
- избирательно и обоснованно распределить доступ к документам и информации между работниками предприятия;
- контролировать знание работниками требований нормативно – методических документов по защите информации и сохранению тайны;
- организовать порядок уничтожения информации;
- своевременно выявлять нарушения требований разрешительной системы доступа работниками предприятия.

5.5.2 Защита персональных данных сотрудников на ОВТи и электронных носителях информации.

Все папки, программы и иные вычислительные комплексы, используемые предприятием и содержащие персональные данные сотрудников, должны быть защищены паролем.

Съемные носители информации на магнитной или оптической основе, в зависимости от характера или длительности использования, допускается учитывать совместно с другими документами по установленным для этого учетным формам. При этом, перед выполнением работ сотрудником, ответственным за размещение на этих носителях информации, предварительно

проставляются любым доступным способом следующие учетные реквизиты: учетный номер и дата, пометки «ДСП», «ПДН» и др., номер экземпляра, подпись этого сотрудника, а также возможные реквизиты идентифицирующие носитель информации.

Носители информации на магнитной (магнитно – оптической), оптической или бумажной основе должны учитываться, хранится и уничтожатся в подразделениях в установленном порядке.

5.6 «Внешняя защита».

5.6.1 Для обеспечения внешней защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица и (или) группы лиц, пытающихся совершить несанкционированный доступ к информации. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.6.2 Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности предприятия, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов на предприятии.

5.6.3 Для обеспечения внешней защиты ПДи существует следующий порядок:

- учет и порядок выдачи пропусков;
- технические средства охраны, сигнализации;
- порядок охраны помещений, транспортных средств.

5.7 Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников (приложение №___).

5.8 По возможности персональные данные обезличиваются.

5.9.Более детально классификация потенциальных нарушителей, оценка исходного уровня защищенности, анализ угроз безопасности персональных данных (описание, оценка вероятности возникновения и опасности угроз, а также меры защиты для уменьшения опасности актуальных угроз) разработаны и утверждены приказом генерального директора в Модели угроз безопасности персональных данных АО «ННПО имени М.В.Фрунзе».

6. Права и обязанности работников предприятия

6.1 Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

6.2 Работники предприятия обязаны ознакомится под роспись с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

6.3 В целях защиты персональных данных, хранящихся на предприятии, работники имеют право на:

6.3.1 полную информацию об их персональных данных и обработке этих данных;

6.3.2 свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных Федеральными законами;

6.3.3 определение своих представителей для защиты своих персональных данных;

6.3.4. доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

6.3.5 исключение или исправление по их требованию неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса или иного Федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

6.3.6 извещение работодателем по их требованию всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех производственных в них исключениях, исправлениях или дополнениях;

6.3.7 обжалование в суде любых неправомерных действий или бездействий работодателя при обработке и защите его персональных данных.

6.4 Работники предприятия обязаны:

- передавать предприятию или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом и иным нормативно – правовыми актами Российской Федерации.

- своевременно сообщать об изменении своих персональных данных (фамилии, имени, отчества, даты рождения, образовании, профессии, специальности), а также об изменениях персональных данных своих работников.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

7.1 Работники предприятия несут персональную ответственность за разглашение конфиденциальной информации, связанной с персональными данными.

7.2 Юридические и физические лица, в соответствии со своими полномочиями, владеющие информацией о гражданах, получающие и использующие ее в рамках деятельности предприятия, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.3 Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.4 Каждый сотрудник предприятия, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность хранящейся на нем информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с Федеральными законами.

7.5.1 За неисполнение или ненадлежащее исполнение работником предприятия по их вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера, предприятие вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

7.5.2 Должностные лица предприятия, в обязанность которых входит ведение и (или) хранение персональных данных работника предприятия, обязаны обеспечить каждому такому работнику возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.5.3 В соответствии с Гражданским Кодексом Российской Федерации лица, незаконными методами получившие информацию, составляющую конфиденциальную информацию, связанную с персональными данными, обязаны возместить причиненные убытки.

7.5.4 Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наступает в соответствии с действующим законодательством РФ.