

УТВЕРЖДАЮ
Генеральный директор
ФГУП СПО «Аналитприбор»

_____ **В.Н. Антонов**

«_____» _____ 2016 г.

*Мотивированное мнение выборного органа
первичной профсоюзной организации №36П/117
(протокол от 25.04.2016 г. № 118) учтено*

ПОЛОЖЕНИЕ
об организации работы с персональными данными

*Вводится в действие с 01.05.2016 г.
в соответствии с приказом от 29.04.2016 г. №94/2*

I. Общие положения

1.1. Настоящее Положение (далее – Положение) определяет основные требования к порядку сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения (далее – обработка) персональных данных работников федерального государственного унитарного предприятия "Смоленское производственное объединение "Аналитприбор" (ФГУП "СПО "Аналитприбор").

1.2. Настоящее Положение разработано на основании статей 23 и 24 Конституции РФ, главы 14 Трудового кодекса РФ, Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", и других нормативных правовых актов Российской Федерации.

1.3. Настоящее Положение утверждается и вводится в действие приказом генерального директора и является обязательным для исполнения всеми работниками предприятия.

1.4. Настоящим Положением определяется порядок обработки персональных данных работников, политика ФГУП «СПО «Аналитприбор» в области обработки персональных данных.

II. Понятие и состав персональных данных

2.1. Персональные данные – любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.2. В состав персональных данных работника входят:

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;

- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате;
- сведения о социальных льготах;
- занимаемая должность;
- адрес места жительства;
- контактная информация (номера домашних, рабочих стационарных (проводных) телефонов, номера мобильных (беспроводных) телефонов, адреса электронной почты), другие средства коммуникации;
- место работы или учебы членов семьи и родственников;
- изображение (фотография);
- иная информация, позволяющая идентифицировать конкретного работника, и необходимая работодателю в связи с трудовыми отношениями.

2.3. Документы, характер информации в которых предполагает или допускает включение в них персональных данных:

- трудовой договор;
- личная карточка работника (форма Т-2);
- личный листок по учету кадров;
- дополнение к личному листку по учету кадров;
- автобиография;
- постоянный пропуск;
- личные дела и трудовые книжки сотрудников;
- приказы по личному составу;
- основания к приказам по личному составу;
- документы о повышении квалификации и переподготовке сотрудников, их аттестации;
- иные документы.

III. Политика в отношении обработки персональных данных

Политика ФГУП «СПО «Аналитприбор» в отношении обработки персональных данных строится на следующих базовых принципах:

3.1. Законность – обработка персональных данных основывается на положениях и требованиях существующих законов, других нормативно-правовых актов и нормативно-методических документов по защите персональных данных, учитывает лучшие мировые практики.

3.2. Системность – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

3.3. Комплексность – безопасность персональных данных обеспечивается комплексом административно-правовых, организационно-технических, физических мер, применение которых обеспечивает предотвращение всех существенных (значимых) каналов реализации угроз безопасности персональных данных.

3.4. Непрерывность – защита персональных данных обеспечивается на всех технологических этапах обработки персональных данных и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

3.5. Своевременность – принимаемые меры по обеспечению безопасности персональных данных носят упреждающий характер. Необходимые меры по защите персональных данных должны приниматься преимущественно до начала их обработки и должны обеспечить надлежащий уровень безопасности персональных данных.

3.6. Преемственность и непрерывность совершенствования – предполагает постоянное совершенствование мер и средств защиты персональных данных на основе результатов анализа функционирования мер по защите персональных данных с учетом отечественного и зарубежного положительного опыта в сфере защиты информации.

3.7. Разумная достаточность и адекватность – состояние и стоимость реализации мер защиты должно быть соизмеримы с рисками, связанными с обработкой и характером защищаемых персональных данных.

3.8. Персональная ответственность – ответственность за обеспечение безопасности персональных данных возлагается на каждого сотрудника предприятия, допущенного к обработке персональных данных в пределах его полномочий.

3.9. Минимизация полномочий – предоставление и использование прав доступа к персональным данным ограничено и управляемо. Доступ к персональным данным предоставляется только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей. Пользователю запрещены все операции с персональными данными за исключением тех, которые разрешены явно.

3.10. Гибкость – в процессе деятельности предприятия могут меняться характеристики, а также объем и категория обрабатываемых персональных данных.

3.11. Открытость алгоритмов и механизмов защиты – защита персональных данных не должна осуществляться только за счет сокрытия структуры, технологий и алгоритмов функционирования принимаемых мер по защите персональных данных, а знание указанных характеристик не должно давать возможности преодоления защиты возможными нарушителями безопасности персональных данных, включая разработчиков средств защиты.

3.12. Научная обоснованность и техническая реализуемость – уровень требований к защите персональных данных соответствует имеющемуся уровню развития информационных технологий и средств защиты информации.

3.13. Специализация и профессионализм – реализация мер по обеспечению безопасности персональных данных осуществляется сотрудниками предприятия, имеющими необходимые навыки и умения.

3.14. Знание работников – предприятие реализует кадровую политику (тщательный подбор персонала и мотивация работников), позволяющую исключить или минимизировать возможность нарушения безопасности персональных данных своими работниками.

3.16. Обязательность контроля и оценки – неотъемлемой частью работ по защите является оценка эффективности системы защиты.

IV. Обработка персональных данных

4.1. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систе-

матизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

4.2. Обработка персональных данных работников осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, а также обеспечения личной безопасности работников, сохранности имущества, контроля количества и качества выполняемой работы.

4.3. Объем обрабатываемых персональных данных определяется ФГУП «СПО «Аналитприбор» исходя из принципа достаточности для целей обработки тех или иных персональных данных.

4.4. Все персональные данные предоставляются работником. 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. Работнику должно быть сообщено о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

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

4.5. Чтобы обеспечить достоверность персональных данных, работник обязан предоставлять работодателю сведения о себе. В случае изменения сведений, составляющих персональные данные (фамилия, имя, отчество, адрес, паспортные данные, сведения об образовании, состоянии здоровья (при выявлении противопоказаний для выполнения работы, обусловленной трудовым договором) и т.п.), работник обязан своевременно предоставлять документы, подтверждающие названные изменения в отдела кадров. Для сведений, не представляющих угрозу жизни и здоровья работника, - такой срок не должен превышать 5 рабочих дней.

4.6. Не допускается получение персональных данных работника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ.

4.7. 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 письменного согласия работника.

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

4.9. Персональные данные не могут быть использованы 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 и карается в соответствии с законодательством РФ.

4.10. Обработка таких персональных данных как изображение (фотография) работника осуществляется с учетом требований приказа по ФГУП «СПО «Аналитприбор»

от 02.10.2013 г. №279 «О порядке обработки некоторых персональных данных работников предприятия».

4.11. Должностные лица (категории сотрудников) ФГУП «СПО «Аналитприбор», имеющие доступ к персональным данным работников, а также персональные данные, к которым они допускаются, определены приложением №1 к настоящему Положению. В отношении подразделений, не все работники которых имеют доступ к персональным данным, конкретные должности лиц, допущенных к работе с ними, определяются отдельным приказом по предприятию (за исключением руководителей и заместителей руководителей соответствующих подразделений).

В случае, если какому-либо должностному лицу, не включенному в данный перечень, требуется для исполнения трудовых (должностных) обязанностей доступ к тем или иным персональным данным работников, то такой доступ осуществляется:

- разовый – на основании служебной записки руководителя соответствующего структурного подразделения с резолюцией о допуске генерального директора;
- постоянный – путем внесения дополнений в утвержденный перечень.

4.12. Доступ к персональным данным допускается после уведомления сотрудника о доступе к персональным данным, ознакомления его с законодательством РФ, регламентирующем вопросы защиты персональных данных и локальными нормативными актами ФГУП «СПО «Аналитприбор» в этой сфере, а также после получения от сотрудника обязательства о неразглашении персональных данных по форме согласно приложению №2 к настоящему Положению.

4.13. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством. Передача персональных данных работников осуществляется в соответствии с требованиями приказа по ФГУП «СПО «Аналитприбор» от 15.09.2014 г. №244 «О передаче персональных данных работников».

4.14. При передаче персональных данных работника работодатель должен 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 федеральным законом;

- 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 секретности (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 локальным нормативным актом ФГУП «Аналитприбор», при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

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

4.15. 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.

4.16. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы организации работодатель не должен 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 федеральным законом.

4.17. Все меры конфиденциальности обработке персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

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

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

Личные дела работников, включая заявление о приеме на работу, трудовой договор, копию приказа о приеме на работу, личный листок по учету кадров с фотографией работника, автобиографию, копию документов об образовании, копию страхового свидетельства государственного пенсионного страхования, копию свидетельства о постановке на учет в налоговый орган и присвоении ИНН, дополнение к личному листку по учету кадров, хранятся в отделе кадров в специально оборудованных шкафах в алфавитном порядке согласно их номерам.

После увольнения работника в личное дело вносятся соответствующие документы (заявление о расторжении трудового договора, копия приказа о расторжении трудового договора), составляется окончательная опись, само личное дело оформляется и передается для хранения в архив предприятия.

Трудовые книжки работников хранятся в отделе кадров в сейфе.

Хранение иных документов, содержащих персональные данные, если иное не установлено локальными нормативными актами предприятия, осуществляется в подразделении, осуществляющим работу с данными документами или использующем их в своей работе в условиях, препятствующих несанкционированному доступу к документам (шкафах, ящиках столов, сейфах и т.п.).

4.20. Исходные файлы документов, содержащие персональные данные в форматах .doc, .docx, .xls, .pdf и т.п., должны храниться на персональных компьютерах исполнителей или серверах, защищенных от несанкционированного доступа паролем, в архивах или файлах, на которых также должен быть установлен пароль. Сведениями об установленных паролях на соответствующих архивах (файлах) обладают исключительно пользователи ПК, которым в силу должностных обязанностей требуется работа с соответствующими документами, а также руководители соответствующих структурных подразделений (лица, их замещающие), начальник ОАСУПиИТ.

Пароль на соответствующих архивах (файлах) должен меняться не реже одного раза в полгода, а при установлении попыток неправомерного доступа к компьютеру, - незамедлительно.

Срок хранения исходных файлов в электронном виде равен сроку хранения соответствующих документов на бумажном носителе, если иное не оговорено законодательством РФ, субъектов РФ, органов местного самоуправления, либо иными локальными нормативными актами ФГУП «СПО «Аналитприбор».

4.21. Срок хранения соответствующих документов на бумажном носителе и в электронном виде не должен превышать срока, необходимого для достижения соответствующих целей обработки персональных данных, если иное не установлено законодательством РФ, субъектов РФ, органов местного самоуправления, например: для целей определения базы по налогам и сборам, для защиты интересов предприятия вследствие признания договора оспоримым или ничтожным.

При обезличивании персональных данных допускается хранение документов неограниченное количество времени.

4.22. Обезличивание или уничтожение документов, в том числе в электронном виде, осуществляется комиссионно. Если иное не оговорено отдельным локальным нормативным актом в состав комиссии входят:

- для бумажных документов: руководитель структурного подразделения, осуществляющего хранение документа, начальник отдела кадров, начальник спецотдела;

- для электронных документов: руководитель структурного подразделения, осуществляющего хранение документа, пользователь ПК, на котором хранился документ, начальник ОАСУПиИТ.

V. Защита персональных данных

5.1. Под угрозой или опасностью утраты персональных данных понимается 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.

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 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 компании.

5.4. Защита персональных данных работника от неправомерного их использования или утраты обеспечивается ФГУП «СПО «Аналитприбор» за счет средств предприятия в порядке, установленном федеральными законами, настоящим Положением, Положением об обработке персональных данных в информационной системе ФГУП «СПО «Аналитприбор», другими локальными нормативными актами.

5.5. Защита персональных данных обеспечивается комплексом административно-правовых, организационно-технических, физических мер, в число которых в том числе входят:

- организация контрольно-пропускного порядка, препятствующего неправомерному проходу на территорию предприятия посторонних лиц;

- обезличения персональных данных по мере возможности;

- защита информации путем двухуровневой системы паролей и установления антивирусных программ;

- ограничение доступа к документам и информации, содержащим персональные данные, в том числе путем хранения их в специальных помещениях, шкафах, сейфах, регламентации должностных обязанностей сотрудников и т.п..

5.6. Начальник отдела кадров осуществляет общий контроль соблюдения мер по защите персональных данных, обеспечивает ознакомление работников под роспись с локальными нормативными актами, а также истребование с работников обязательств о неразглашении персональных данных.

5.7. Начальник отдела автоматизированной системы управления производством и информационных технологий отвечает за обеспечение безопасности персональных данных, содержащихся в информационной системе предприятия.

VI Права и обязанности работника

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

6.2. Работники и их представители должны быть ознакомлены под роспись с настоящим Положением, а также касающимися их деятельности локальными нормативными актами ФГУП «СПО «Аналитприбор» в области обработки и защиты персональных данных.

6.3. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работник имеет право:

- получать полную информацию о своих персональных данных и обработке этих данных;

- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законом;

- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением федерального закона. Работник при отказе работодателя исключить или исправить персональные данные работника имеет право заявлять в письменной форме работодателю о своём несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

- требовать от работодателя уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведённых в них изменениях или исключениях из них;

- обжаловать в суд неправомерные действия или бездействие работодателя при обработке персональных данных.

6.4. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;

- своевременно сообщать работодателю об изменении своих персональных данных;

6.5. Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании пред-

ставленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

6.6. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

VII Ответственность за разглашение персональных данных

7.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут персональную материальную, дисциплинарную, административную, гражданско-правовую и/или уголовную ответственность в порядке, установленном действующим законодательством Российской Федерации.

7.2. Сотрудники, имеющие доступ к персональным данным работника и совершившие указанный дисциплинарный проступок, несут полную материальную ответственность в случае причинения его действиями ущерба работодателю (п.7 ст. 243 Трудового кодекса РФ).

7.3. Должностные лица, в обязанность которых входит обработка персональных данных сотрудника, обязаны обеспечить каждому 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.

7.4. Разглашение персональных данных работника (передача их посторонним лицам, в том числе работникам ФГУП "СПО "Аналитприбор", не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные работника, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарного взыскания.

**Обязательство
о неразглашении персональных данных**

Я,					
	(фамилия, имя, отчество)				
паспорт:				выдан	
	(серия)		(номер)		(наименование учреждения, выдавшего паспорт)
дата выдачи			, работающий в		
					(наименование структурного подразделения)
в должности					,
	(наименование должности)				
уведомлен о том, что получаю доступ к персональным данным сотрудников (ненужное вычеркнуть):					

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате;
- сведения о социальных льготах;
- занимаемая должность;
- адрес места жительства;
- контактная информация (номера домашних, рабочих стационарных (проводных) телефонов, номера мобильных (беспроводных) телефонов, адреса электронной почты), другие средства коммуникации;
- место работы или учебы членов семьи и родственников;
- изображение (фотография);
- иная информация, позволяющая идентифицировать конкретного работника, и необходимая работодателю в связи с трудовыми отношениями.

Получая доступ к указанным персональным данным, я понимаю, что при исполнении своих должностных обязанностей, буду заниматься их сбором, обработкой и хранением.

Я понимаю, что разглашение такого рода информации может нанести как прямой, так и косвенный ущерб сотрудникам предприятия.

В связи с этим, даю обязательство, при работе с персональными данными соблюдать требования действующего законодательства Российской Федерации и локальных нормативных актов ФГУП «СПО «Аналитприбор». Я подтверждаю, что без письменного согласия субъекта персональных данных, не имею права разглашать персональные данные и передавать их третьим лицам.

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных сотрудника или их утраты я несу ответственность в соответствии со ст. 90 Трудового Кодекса РФ, ст. 24. Федерального Закона РФ "О персональных данных".

Со статьями 23 и 24 Конституции РФ, главой 14 Трудового кодекса РФ, Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", "Положением об организации работы с персональными данными", «Положением об обработке персональных данных в информационной системе ФГУП «СПО «Аналитприбор» ознакомлен (а).

« » 20 г.

(подпись)

(фамилия, имя, отчество)