Приложение №1
к приказу от «29» 01 2019 г.
№ 01-01/12

ПОЛИТИКА
АО «ВНИИСВ» В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Введение.

Обеспечение конфиденциальности и безопасности обработки персональных данных в АО «ВНИИСВ» является одной из приоритетных задач организации.

В АО «ВНИИСВ» для этих целей введен в действие комплект организационно-распорядительной документации, обязательный к исполнению всеми сотрудниками компании, допущенными к обработке персональных данных.

Обработка, хранение и обеспечение конфиденциальности и безопасности персональных данных осуществляется в соответствии с действующим законодательством РФ в сфере защиты персональных данных, и в соответствии с локальными актами АО «ВНИИСВ».

Настоящая Политика определяет принципы, порядок и условия обработки персональных данных работников АО «ВНИИСВ» и иных лиц, чьи персональные данные обрабатываются организацией, с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также устанавливает ответственность должностных лиц АО «ВНИИСВ», имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2. Понятие и состав персональных данных.

Перечень персональных данных, подлежащих защите в АО «ВНИИСВ» определятся Федеральным законом «О защите персональных данных», Трудовым кодексом РФ и другими нормативно-правовыми актами.

Сведениями, составляющими персональные данные, в АО «ВНИИСВ» является любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

3. Цели обработки персональных данных.

АО «ВНИИСВ» осуществляет обработку персональных данных в следующих целях:

- организации кадрового учета компании,
- обеспечения соблюдения законов и иных нормативно-правовых актов;
- ведения кадрового делопроизводства
- исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога;
- пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации
- в соответствии с Трудовым кодексом РФ, Налоговым кодексом РФ, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных» и других нормативно-правовых актов.

4. Сроки обработки персональных данных.

Сроки обработки персональных данных определяются в соответствие со сроком действия договора (соглашением) с субъектом персональных данных.

В АО «ВНИИСВ» создаются и хранятся документы, содержащие сведения о субъектах персональных данных. Требования к использованию в АО «ВНИИСВ» данных типовых форм документов установлены Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5. Права и обязанности.

АО «ВНИИСВ» как оператор персональных данных в праве:

- отстаивать свои интересы в суде;

- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
- отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;
- использовать персональные данные субъекта без его согласия, в случаях, предусмотренных законодательством.

Субъект персональных данных имеет право:

- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- требовать перечень своих персональных данных, обрабатываемых АО «ВНИИСВ» и источник их получения;
- получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;
- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

6. Принципы и условия обработки персональных данных.

Обработка персональных данных в АО «ВНИИСВ» производится на основе соблюдения принципов:

- законности целей и способов обработки персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;
- хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;
- уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

Отказ клиента АО «ВНИИСВ» от предоставления согласия на обработку его персональных данных влечет за собой невозможность достижения целей обработки.

7. Обеспечение безопасности персональных данных.

АО «ВНИИСВ» предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

В целях координации действий по обеспечению безопасности персональных данных в АО «ВНИИСВ» назначен ответственный за организацию защиты персональных данных.

8. Заключительные положения.

Настоящая Политика предназначена для размещения в информационных ресурсах общественного пользования АО «ВНИИСВ».

Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных АО «ВНИИСВ».

Ответственность должностных лиц АО «ВНИИСВ», имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с

законодательством Российской Федерации и внутренними документами АО «ВНИИСВ».

Приложение №2
к приказу от «____»_____2019 г.
№ _____

ПОЛОЖЕНИЕ
Об обработке и защите персональных данных в АО «ВНИИСВ»

1. Общие положения

1.1. Целью данного Положения является защита персональных данных от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, Федерального закона «Об информации, информатизации и защите информации», Федерального закона «О персональных данных» и других нормативно-правовых документов.

1.4. Настоящее Положение утверждается и вводится в действие приказом временного генерального директора и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

2. Понятие и состав персональных данных

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу.

2.2. Состав персональных данных, обрабатываемых в АО «ВНИИСВ».

3. Права субъекта персональных данных

Субъект имеет право:

3.1. На полную информацию о своих персональных данных и обработке этих данных.

3.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных законодательством РФ.

3.3. Требовать об исключении или исправлении неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований, определенных законодательством РФ.

3.4. Обжаловать в суде любые неправомерные действия или бездействие АО «ВНИИСВ» при обработке и защите его персональных данных.

4. Передача персональных данных

4.1. При передаче персональных данных АО «ВНИИСВ» должна соблюдать следующие требования:

- передавать персональные данные только тем организациям, с которыми заключен договор с указанием обязанности обеспечивать защиту информации, являющейся государственным информационным ресурсом в соответствии с текущим законодательством РФ.

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

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

- передавать персональные данные в порядке, установленном законодательством РФ, и ограничивать передаваемую информацию только теми персональными данными, которые необходимы для выполнения конкретных функций.

5. Доступ к персональным данным работников

5.1. Параметры доступа к персональным данным описаны в документе «Положение о разграничении прав доступа к защищаемой информации».

6. Защита персональных данных работников

6.1. В целях обеспечения сохранности и конфиденциальности персональных данных все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только сотрудниками АО «ВНИИСВ».

6.2. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной

форме на бланке организации и в том объеме, который позволяет не разглашать излишний объем персональных сведений о субъектах персональных данных.

6.3. Личные дела и документы, содержащие персональные данные, хранятся в запирающихся шкафах, обеспечивающих защиту от несанкционированного доступа.

6.4. Персональные компьютеры, в которых содержатся персональные данные работников, должны быть защищены в соответствии с требованиями нормативных документов по защите информации.

7. Ответственность за разглашение персональных данных работников

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

Приложение №3
к приказу от «____»_____2019 г.
№ _____

Перечень информационных систем персональных данных
в АО «ВНИИСВ»

В соответствии с Федеральным законом № 152-ФЗ «О персональных данных» в АО «ВНИИСВ» выделены следующие информационные системы персональных данных (ИСПДн):

Наименование ИСПДн	Категория субъектов персональных данных	Расположение элементов ИСПДн	Уровень защищенности ИСПДн
УПП 1С	Сотрудники оператора ИСПДн	Полностью на территории РФ	4-УЗ

Приложение №4
к приказу от «____»_____2019 г.
№ _____

ПЕРЕЧЕНЬ
сведений конфиденциального характера в АО «ВНИИСВ»

В АО «ВНИИСВ» присутствуют следующие сведения конфиденциального характера:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

3. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

Приложение №5
к приказу от «____»_____2019 г.
№ _____

ПЕРЕЧЕНЬ

персональных данных, подлежащих защите

Персональные данные {субъекты персональных данных}:

- фамилия,
- имя,
- отчество;
- дата рождения;
- пол;
- паспортные данные;
- домашний адрес;
- сведения о составе семьи:
- фамилии, имена, отчества родителей (законных представителей);
- место работы;
- занимаемая должность;
- контактные телефоны;
- сведения о воинской обязанности;
- образование;
- владение иностранными языками;
- учёная степень;
- научные труды и изобретения;
- выполняемая работа;
- факты пребывания за границей;
- участие в выборных органах;
- изучаемая специальность;
- данные приказа о зачислении.

Приложение №6

к приказу от «____»_____2019 г.

№ _____

ПОРЯДОК
резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации ИСПДн «УПП 1С»

1. Назначение и область действия

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия, связанные с функционированием ИСПДн «УПП 1С», меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери.

Задачи, решаемые данной Инструкции, охватывают определение мер защиты от потери информации; определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей ИСПДн, имеющих доступ к ее ресурсам, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе: системы жизнеобеспечения; системы обеспечения отказоустойчивости; системы резервного копирования и хранения данных; системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор безопасности информации.

Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор безопасности информации.

2. Порядок реагирования на инцидент

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти: в результате непреднамеренных действий пользователей; в результате преднамеренных действий пользователей и третьих лиц; в результате нарушения правил эксплуатации технических средств ИСПДн; в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале учета мероприятий по контролю обеспечения защиты информации в ИСПДн «УПП 1С».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники АО «ВНИИСВ» предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. Технические меры.

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как системы жизнеобеспечения; системы обеспечения отказоустойчивости; системы резервного копирования и хранения данных; системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают: пожарные сигнализации и системы пожаротушения; системы вентиляции и кондиционирования; системы резервного питания.

Все критичные помещения АО «ВНИИСВ» (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и (или) пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания (или встроенные аккумуляторы). В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

– локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

– источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

– дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

– резервные линии электропитания в пределах комплекса зданий;

– аварийные электрогенераторы.

– системы обеспечения отказоустойчивости:

– кластеризация;

– технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев могут использоваться методы кластеризации, в частном случае территориально удаленные системы кластеров. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.2. Организационные меры

Резервное копирование и хранение данных должно осуществлять на периодической основе - для обрабатываемых персональных данных – не реже раза в неделю; для технологической информации – не реже раза в месяц; эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведении процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Носители, на которые произведено резервное копирование, должны быть пронумерованы и учтены: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

К проекту документа: Приказ от « 29 » 01 2019 г. № 01-01/12

Об утверждении локальных нормативных документов по обработке и защите персональных данных

(наименование документа)

Исполнитель: Главный метролог

(должность)

Е. А. Гуркин

(подпись) (И. О. Фамилия)

Лист согласования:

И.О. Фамилия	Должность	Ответ, полученный от согласующего Согласовано / замечания прилагаются
С. В. Коломийцев	Первый заместитель генерального директора	
О. Б Шведов	Начальник департамента безопасности и режима	

Заключение о готовности к подписанию: _____

(заполняется секретарем директора)

Инициатор: Главный метролог _____ Е. А. Гуркин

(должность) (подпись) (И.О. Фамилия)