УТВЕРЖДАЮ ГЕНЕРАЛЬНЫЙ ДИРЕКТОР

ОАО «КОНЦЕРН «НПО «АВРОРА»

п/п К.Ю. Шилов

« 02 » ноября 2012 г.

# Политика информационной безопасности персональных данных ОАО "Концерн "НПО "Аврора"

**Содержание**

## 1 Область применения

Политика информационной безопасности персональных данных (далее Политика) предназначена для ознакомления работников с позицией Общества в отношении защиты персональных данных. В Политике рассматриваются правовые, организационные и технические вопросы, связанные с обработкой и защитой персональных данных работников Общества.

Руководители подразделений обязаны ознакомить своих работников с данной Политикой под роспись. Вновь принятые работники должны быть ознакомлены с Политикой в Отделе кадров при приёме на работу.

## 2 Сокращения

АС – автоматизированная система

БД – база данных

ИСПДн – информационная система персональных данных

КСП – корпоративная сеть предприятия

НСД – несанкционированный доступ

ОС – операционная система

ПД – персональные данные

ПО – программное обеспечение

ПрК – пронзводственный комплекс

ТК РФ – трудовой кодекс Росснйской Федерации

ФСТЭК – Федеральная служба по техническому и экспортному контролю

ЦП – центральная площадка

## 3 Определения

**Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

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

**Аутентификация** - процедура проверки подлинности субъекта доступа;

**Безопасность информации (данных)** - состояние защищённости информации (данных), при котором обеспечены её (их) конфиденциальность, доступность и целостность;

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

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

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

**Доступ к информации** - ознакомление с ней, её обработка, в частности копирование, модификация и уничтожение. Понятие доступа к информации неразрывно связано с понятиями субъекта и объекта доступа;

**Доступность** - свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц;

**Защита персональных данных** - комплекс мероприятий технического, организационного и организационно-технического характера, направленных

на защиту сведений, относящихся к определённому или определяемому на основании такой информации физическому лицу;

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

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

**Информационная система персональных данных** - совокупность содержащихся в БД персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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

**Компьютерный вирус** — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация);

**Конфиденциальность** - свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц;

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

**Неавтоматизированная обработка персональных данных** – обработка персональных данных считается осуществлённой без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение осуществляются при непосредственном участии человека;

**Несанкционированный доступ к информации** – доступ, нарушающий установленные правила разграничения доступа. Субъект, осуществляющий несанкционированный доступ, является нарушителем правил разграничения

доступа. Несанкционированный доступ является наиболее распространённым видом нарушений безопасности информации;

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

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

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

**Общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

**Объект доступа** – пассивный компонент системы, хранящий, принимающий или передающий информацию (файл, каталог и т.п.);

**Оператор персональных данных** - 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;

**Перехват информации** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов;

**Персональные данные** - любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных);

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

**Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределённому кругу лиц;

**Санкционированный доступ к информации** – это доступ, не нарушающий установленные правила разграничения доступа, служащие для регламентации прав доступа субъектов к объектам доступа;

**Специальные категории персональных данных** - персональные данные, касающиеся расовой принадлежности, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

**Субъект доступа** – это активный компонент системы, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы (пользователь, процесс, прикладная программа и т.п.);

**Угрозы безопасности персональных данных** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование;

**Уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

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

**Уязвимость информационной системы персональных данных** - недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении ИСПД, которые могут быть использованы для реализации угрозы безопасности персональных данным;

**Целостность** - неизменность информации в процессе её передачи или хранения

## 4 Правовые аспекты защиты персональных данных

### 4.1 Перечень нормативных документов

Обработка и защита персональных данных в ОАО «Концерн «НПО «Аврора» организована в соответствии с требованиями Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персоиальных данных», Федерального закона от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в иформационных системах персональных данных», приказа Минкультуры Российской Федерации от 25 августа 2010 г. № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», а также норматнвных документов ФСТЭК России.

### 4.2 Права работников Общества на защиту своих персональных данных

В соответствии со ст. 89 ТК РФ работники имеют право:

- получать полную информацию об их персональных данных и обработке этих данных;

- получать свободный бесплатный доступ к своим персональным данным, в т.ч. получать копию любой записи, содержащей такие данные;

- требовать от работодателя известить всех лиц, которым ранее были сообщены неверные или неполные персональные данные этого работника, обо всех произведёиных в них исключениях, исправлениях или дополнениях;

- обжаловать в суде любые неправомерные действия или бездействие работодателя при обработке и защите его персональных данных;

- определять представителя для защиты своих персональных данных;

- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушениями

требований ТК РФ или иного федерального закона. В случае отказа работодателя исключить или исправить персональные данные работника, последний имеет право заявить в письменной форме работодателю о своём несогласии с соответствующим обоснованием.

В соответствии с п. 4 ст. 86 ТК РФ работодатель не имеет права получать и обрабатывать данные работника о его политических, религиозных и иных убеждениях и частной жизни без его письменного согласия, если это не связано с трудовыми отношениями. Неприкосновенность частной жизни гарантирована ст. 23 Конституции РФ, и согласно ст. 24 Конституции сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

В соответствии с п. 8 ст. 86 ТК РФ работники и их представители должны быть ознакомлены под роспись с документами, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

В соответствии со ст. 62 ТК РФ, по письменному заявлению работника работодатель обязан не позднее трёх рабочих дней со дня получения от работника заявления выдать ему копии документов, связанных с работой (приказа о приёме на работу, приказов о переводах на другую работу, приказа об увольнении с работы, выписки из трудовой книжки, справок о заработной плате, о начисленных и фактически уплаченных пенсионных взносах, о периоде работы у данного работодателя и т.д.). Данные копии заверяются надлежащим образом и предоставляются работнику безвозмездно.

**4.3 Цели обработки и состав обрабатываемых персональных данных**

Цели обработки персональных данных работников Общества: кадровый учёт и расчёт заработной платы работников.

В Обществе определён следующий перечень персональных данных работников, подлежащих обработке:

- фамилия, имя, отчество;

- паспортные данные;

- дата и место рождения;

- пол;

- код ИФНС;

- ИНН;

- № ПФР;

- адрес по прописке;

- фактический адрес;

- телефон;

- гражданство;

- сведения о воинском учёте;

- сведения о родственниках (ФИО и дата рождения);

- семейное положение;

- образование;

- знание иностранных языков;

- членство в профсоюзе;

- налоговый статус (резидент/не резидент);

- должность и подразделение;

- трудовая деятельность;

- сведения о заработной плате;

- режим труда;

- данные по медицинскому страхованию и т.д.

**4.4 Период хранения персональных данных работников**

В соответствии с Приказом Минкультуры РФ от 25.08.2010 N 558 сведения о персональных данных работников Общества относятся к документам долговременного хранения и сроки их хранения составляют 75 лет или постоянно. Личные дела руководителя организации, членов руководящих, исполнительных, контрольных органов, работников, имеющих государственные и иные звания, премии, награды, степени и звания, хранятся постоянно, а иных работников - в течение 75 лет. Трудовые договоры, соглашения, не вошедшие в состав личных дел, должны храниться 75 лет.

Также 75 лет хранятся личные карточки. Невостребованные трудовые книжки хранятся 75 лет.

## 5 Технические меры обеспечения защиты персоиальных данных

В Обществе приняты следующие технические меры для защиты персональных данных работников:

### 5.1 Выделениая компьютерная сеть

Компьютерная сеть, в которой производится обработка персональных данных работников Общества (Сеть службы управления персоналом) физически отделена от других компьютерных сетей. Таким образом, ИСПДн полностью защищена от угроз проникновения из сетей общего пользования, как из сети Интернет, так и из КСП.

Данные из Сети службы управления персоналом могут быть переданы на сменном носителе информации или в каком-либо другом виде в следующих случаях:

- если эти данные объявлены общедоступными (согласие на общедоступность было дано работником в письменном виде) ;

- в случаях, предусмотреиных ТК РФ или иными Федеральными законами;

- в случае, когда работник запрашивает свои персональные данные либо специально предоставляет письменное разрешение на их передачу

### 5.2 Сертифицированное программное обеспечение

На компьютерах ИСПДн установлено сертифицированное ФСТЭК программное обеспечение (операционные системы семейства Windows) и электронные ключи доступа eToken, также сертифицированные ФСТЭК. Использование сертифицированного ПО гарантирует отсутствие недекларированных возможностей, которые могут привести к утечке, блокированию либо уничтожению информации.

### 5.3 Система резервного копирования и восстановления данных

Для обеспечеиия целостности и доступности персональных данных работников Общества разработана система резервного копирования и восстановления баз данных ИСПДн.

Резервное копирование на основной и вспомогательный сервер ИСПДн осуществляется ежедневно. Кроме того, раз в месяц создаются резервные

копии на сменном носителе информации. Таким образом, заблокированные, утерянные или повреждённые в результате какого-либо сбоя или злонамеренных действий нарушителя персональные данные в любой момент могут быть восстановлены.

### 5.4 Подсистема разграничения доступа и аудита

Разграничение доступа в ИСПДн организовано на нескольких уровнях:

- средствами ОС и Active Directory;

- с помощью электронных ключей доступа (eToken) ;

- средствами ПО, применяемого для обработки ПД

Разграничение доступа организовано таким образом, чтобы каждый пользователь ИСПДн имел доступ только к ресурсам, необходимым ему для исполнения должностных обязанностей. Кроме того, многоуровневая аутентификация максимально затрудняет несанкционированный доступ к персональным данным.

Система аудита также организована как на уровне ОС, так и средствами ПО, применяемого для обработки ПД. Осуществляется регистрация следующих действий пользователей:

- входа\выхода в систему\из системы;

- попыток доступа (успешных и неуспешных) к программным компонентам;

- любых действий с ПД (внесение, изменение, удаление и т.д.), производимых в базе данных

### 5.5 Антивирусная защита

Антивирусная система служит для защиты серверов и компьютеров пользователей от сбоев в работе ОС и функционального ПО, которые могут возникнуть в результате воздействия вирусов.

Антивирусные средства установлены на всех компьютерах ИСПДн и управляются централизованно с единой консоли. С консоли производится установка и настройка клиентов, а также обновление антивирусных баз. Загрузка антивирусных средств производится автоматически при старте

системы, отключение компонентов антивирусной защиты возможно только с центральной консоли управления.

## 6 Организационные меры обеспечения защиты персональных данных

### 6.1 Пользователи ИСПДн

К работе в ИСПДн допущены только пользователи из списка, утверждённого генеральным директором, и ознакомленные с инструкцией по работе со средствами защиты информационной системы персональных данных Сети службы персонала ОАО «Концерн «НПО «Аврора». При необходимости корректировки списка пользователей выпускается соответствующий приказ генерального директора.

### 6.2 Ответственные за обеспечение защиты ИСПДн

Ответственные за обеспечение защиты ИСПДн:

- ответственный за эксплуатацию ИСПДн;

- ответственный за безопасность функционирования средств защиты информации, используемых в ИСПДн;

- ответственный за контроль обеспечения безопасности персональных данных в ИСПДн

Ответственный за эксплуатацию ИСПДн проводит инструктаж работников и обеспечивает контроль выполнения работниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн.

Ответственный за безопасность функционирования средств защиты информации, используемых в ИСПДн, занимается настройкой системы разграничения доступа и аудита, обновлением антивирусного ПО, восстанавливает программную среду в случае сбоев, обеспечивает резервное копирование и восстановление данных и т.д.

Ответственный за контроль обеспечения безопасности персональных данных в ИСПДн контролирует доступ лиц в помещения, где ведётся обработка ПД, проводит работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники и т.д.

Ответственные назначаются приказом генерального директора ОАО «Концерн «НПО «Аврора».

**6.3 Доступ в помещения**

Помещения, в которых производится обработка персональных данных, оборудованы замками на дверях. Ключи от помещения выдаются только работникам, непосредственно в нём работающим, либо ответственным за это помещение. Если работники – пользователи ИСПДн покидают помещение, оно должно быть заперто. Также помещения оборудованы датчиками охранной сигнализации. Постановка на сигнализацию осуществляется в конце рабочего дня работником, работающим в помещение либо ответственным за него.

Работники Общества, непосредственно не занятые обработкой персональных данных, допускаются в помещения, где производится такая обработка, только в сопровождении пользователей ИСПДн. При этом ознакомление таких работников с персональными данными не допускается, за исключением ознакомления с их собственными документами (трудовыми книжками, договорами, приказами о приёме\увольнении и т.п.) исключительно в бумажном виде.

Лица, не являющиеся работниками Общества, не допускаются в помещения, где производится обработка персональных данных. Исключение составляют случаи, предусмотренные законодательством (такие, как проверка работы Общества государственными органами). В этом случае доступ в помещения также осуществляется только в сопровождении пользователей ИСПДн и только после уведомления руководства Общества.

**6.4 Ответственность работников**

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

Пользователь ИСПДн несёт ответственность за все действия, совершённые от имени его учётной записи.

### 6.5 Основные требования к работникам, имеющим доступ к ИСПДн

Для предотвращения несанкционированного доступа к ресурсам ИСПДн пользователям следует:

- соблюдать правила использования пользовательских паролей (назначать индивидуальные пароли как для входа в сеть, так и для входа в БД по работникам Общества; хранить пароли в секрете; изменять пароли при возможной компрометации; выбирать длинные и сложные пароли );

- обеспечивать защиту пользовательского оборудования (осуществлять доступ в помещения согласно п.6.3 Политики; устанавливать блокировку текущего сеанса, если рабочая станция пользователя остаётся без присмотра; завершать активные сеансы по окончании работы);

- при работе с электронными ключами доступа руководствоваться инструкцией по работе со средствами защиты информационной системы персональных данных Сети службы персонала ОАО «Концерн «НПО «Аврора»

- сообщать обо всех угрозах безопасности ИСПДн ответственному за эксплуатацию ИСПДн, ответственному за безопасность функционирования средств защиты информации, используемых в ИСПДн или ответственному за контроль обеспечения безопасности персональных данных в ИСПДн

## 7 Внесение изменений в Политику

Внесение изменений в Политику может быть вызвано:

- изменениями в действующем законодательстве РФ по персональным данным;

- изменениями в структуре ИСПДн;

- изменениями в структуре системы защиты ИСПДн