УТВЕРЖДЕНА
Приказом Генерального директора
АО «ОХК «УРАЛХИМ»
№ П-10/0700/0033-16 от «11» марта 2016 г.

# Политика
# АО «ОХК «УРАЛХИМ»
# в отношении обработки персональных данных

№ П-10/002.1

УРАЛХИМ

АО «ОХК «УРАЛХИМ»
2016

# Оглавление

# 1. Глоссарий

## 1.1. Термины

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

**Безопасность персональных данных** - защищенность персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

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

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

**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) с персональными данными, совершаемых с использованием средств автоматизации или без использования таких средств. К таким действиям (операциям) можно отнести: сбор, получение, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Общество** - Акционерное общество «Объединенная химическая компания «УРАЛХИМ» (АО «ОХК «УРАЛХИМ»), включающее все его структурные подразделения, включая филиалы и представительства.

**Оператор** - Общество, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

**Политика** – настоящая Политика АО «ОХК «УРАЛХИМ» в отношении обработки персональных данных.

**Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

**Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). К такой информации, в частности, можно отнести: ФИО, год, месяц, дата и место рождения, адрес, сведения о семейном, социальном, имущественном положении, сведения об образовании, профессии, доходах, а также другую информацию.

**Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**Субъект персональных данных (Субъект)** - физическое лицо, персональные данные которого обрабатываются.

**Трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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

### 1.2. Сокращения

**АРМ** – автоматизированное рабочее место.

**ИСПДн** - Информационная система персональных данных.

**НСД** – несанкционированный доступ.

**ПДн** - Персональные данные.

## 2. Информация о документе

### 2.1. Назначение

Политика определяет позицию и намерения Общества в области обработки и защиты персональных данных лиц, состоящих в трудовых, гражданско-правовых и иных отношениях с Обществом (далее по тексту – Субъект), соблюдения прав и основных свобод каждого Субъекта и в особенности права на неприкосновенность частной жизни, личную и семейную тайну.

### 2.2. Область применения

Политика предназначена для изучения и неукоснительного исполнения руководителями и работниками всех структурных подразделений Общества, а также подлежит доведению до сведения Субъектов, партнеров и других заинтересованных сторон путем опубликования настоящей Политики в открытых источниках в соответствии с требованиями действующего законодательства.

Для дочерних обществ носит рекомендательный характер, однако, рекомендуется для адаптации и принятия на уровне дочерних и зависимых Обществ.

### 2.3. Порядок утверждения, внесения изменений и дополнений

Политика утверждается и вводится в действие приказом Генерального директора.

Все изменения в Политику вносятся путем утверждения Политики в новой редакции.

Пересмотр положений настоящей Политики проводится периодически не реже чем 1 раз в 3 года, а также:

- при изменении законодательства Российской Федерации в области персональных данных;
- при изменении состава лиц, которым Общество поручает обработку персональных данных;
- в случаях выявления несоответствий, затрагивающих обработку персональных данных;
- по результатам контроля выполнения требований по обработке и защите персональных данных;
- по решению руководства Общества.

## 3. Правовая основа обработки и обеспечения безопасности персональных данных

Обработка и обеспечение безопасности персональных данных в Обществе осуществляется в соответствии с требованиями Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона № 152-ФЗ «О персональных данных», подзаконных актов, других нормативных актов, обязательных к применению.

## 4. Принципы обработки персональных данных

При обработке персональных данных Общество придерживается следующих принципов:

- осуществляет обработку персональных данных только на законной и справедливой основе;
- не раскрывает третьим лицам и не распространяет персональные данные без согласия Субъекта (если иное не предусмотрено действующим законодательством Российской Федерации);
- определяет конкретные законные цели до начала обработки (в т.ч. сбора/получения) персональных данных;
- собирает только те персональные данные, которые являются необходимыми и достаточными для заявленной цели обработки;
- не осуществляет сбор и обработку персональных данных Субъекта, касающихся расовой, национальной принадлежности, политических, религиозных, философских и иных убеждений, состояния здоровья, интимной жизни, членства в общественных объединениях, в том числе в профессиональных союзах;
- обработка персональных данных в Обществе ограничивается достижением конкретных, заранее определенных и законных целей;
- уничтожает либо обезличивает персональные данные по достижении целей обработки или в случае утраты необходимости в достижении целей.

## 5. Субъекты информационных отношений и их интересы

Субъектами информационных отношений при обеспечении безопасности персональных данных Общества являются:

- АО «ОХК «УРАЛХИМ», как Владелец информационных систем ПДн;
- Работники, в соответствии с возложенными на них функциями;
- лица, являющихся соискателями должностей в Обществе;
- Физические лица, состоящие с Обществом в гражданско-правовых отношениях (Субъект).

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- своевременного доступа к необходимым персональным данным (их доступности);
- достоверности (полноты, точности, адекватности, целостности) персональных данных;
- конфиденциальности (сохранения в тайне) персональных данных;
- защиты от навязывания ложных (недостоверных, искаженных) персональных данных;
- разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с персональными данными;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи персональных данных;
- защиты персональных данных от незаконного распространения.

## 6. Цель обеспечения безопасности персональных данных

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита законных интересов Субъектов персональных данных и Общества от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств персональных данных:

- защищенность ПДн от незаконного распространения;
- конфиденциальности - сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи;
- целостности и достоверности персональных данных, хранимых и обрабатываемых в ИСПДн Общества и передаваемой по каналам связи;

- доступности персональных данных для легальных пользователей (устойчивого функционирования ИСПДн Общества, при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время).

Необходимый уровень защищенности, доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

# 7. Задачи обеспечения безопасности персональных данных

## 7.1. Задачи системы обеспечения безопасности персональных данных

Для достижения основной цели защиты и обеспечения указанных свойств ПДн система обеспечения безопасности персональных данных Общества обеспечивает эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем Общества;
- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защита от вмешательства в процесс функционирования информационных систем Общества посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- ограничение доступа пользователей к ИСПн Общества (возможность доступа только к тем системам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- защита от несанкционированной модификации используемых в информационных системах Общества программных средств, а также защита системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защита ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

## 7.2. Пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите ИСПДн (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
- учетом действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационной системы;
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Общества по вопросам обеспечения безопасности информации;
- подготовкой должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;

- наделением работников Общества (пользователи) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Общества;
- непрерывным поддержанием необходимого уровня защищенности ИСПДн Общества;
- применением физических и технических (программно-аппаратных) средств защиты ИСПДн и непрерывной административной поддержкой их использования;
- эффективным контролем над соблюдением пользователями ИСПДн Общества требований по обеспечению безопасности информации;
- юридической защитой интересов Общества и Субъектов ПДн от противоправных действий сторонних организаций и третьих лиц.

# 8. Объекты защиты

Основными объектами системы безопасности персональных данных являются:

- ИСПДн с ограниченным доступом;
- процессы обработки персональных данных в ИСПДн Общества, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки персональных данных.

# 9. Меры по обеспечению требуемого уровня защиты ИСПДн

Все меры обеспечения безопасности ИСПДн Общества подразделяются на:

- правовые (законодательные);
- организационные;
- административные;
- физические;
- технические (аппаратные и программные).

## 9.1. Правовые (законодательные) меры защиты

К правовым мерам защиты относятся действующие нормативные акты, регламентирующие правила обработки персональных данных, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил.

## 9.2. Организационные меры защиты

К данному виду мер защиты относятся разного рода технологические решения и приемы, направленные на уменьшение возможности совершения работниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

## 9.3. Административные меры защиты

Административные меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки персональных данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

### 9.3.1. Регламентация доступа в помещения

Компоненты информационных систем Общества должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, АРМ и т.п.).

Во время обработки персональных данных в таких помещениях должен присутствовать только персонал, допущенный к работе с персональными данными. Запрещается прием посетителей в помещениях, когда осуществляется обработка персональных данных.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

### 9.3.2. Регламентация допуска работников к использованию ИСПДн

В рамках разрешительной системы (матрицы) доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационными системами Общества и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально. Каждый работник пользуется только предписанными ему правами по отношению к персональным данным, с которыми ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с ответственными за организацию обработки персональных данных.

Все работники Общества и обслуживающий персонал, несут персональную ответственность за нарушения установленного порядка обработки персональных данных, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы.

Обработка персональных данных в компонентах информационных систем Общества должна производиться в соответствии с утвержденными технологическими инструкциями.

### 9.3.3. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест работников Общества, с которых возможен доступ к ресурсам информационной системы, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

В компонентах информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

### 9.3.4. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

Оборудование ИСПДн, используемое для доступа и хранения персональных данных, к которому доступ работников Общества в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться.

### 9.3.5. Ответственность за нарушения установленного порядка пользования ресурсами информационных систем Общества

Мера ответственности работников за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с персональными данными, должна определяться в соответствии с требованиями действующего законодательства и локальных нормативных актов Общества.

## 9.4. Физические меры защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания

физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемым персональным данным, а также технических средств визуального наблюдения, связи и охранной сигнализации.

## 9.5. Технические (аппаратно-программные) меры защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности персональных данных по всем направлениям защиты в состав средств защиты ПДн, применяемых в Обществе, могут быть включены средства защиты нижеприведенных категорий. Конкретный перечень технических средств защиты ПДн определяется отдельно для каждой ИСПДн.

### 9.5.1. Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами информационных систем Общества посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

### 9.5.2. Средства разграничения доступа

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

### 9.5.3. Средства оперативного контроля и регистрации событий безопасности

Средства оперативного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации.

### 9.5.4. Средства обеспечения и контроля целостности

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов системы предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации персональных данных должен обеспечиваться:

- средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);
- средствами электронной подписи;
- средствами подсчета контрольных сумм (для используемого программного обеспечения).

# 10. Передача персональных данных

Общество вправе поручить обработку персональных данных (с согласия Субъекта ПДн) юридическим лицам, на основании заключаемого с этим лицом договора, на основании которого указанные лица обязуются соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ «О персональных данных».

В случае осуществления Обществом трансграничной передачи персональных данных Субъекта на территорию иностранного государства указанная трансграничная передача должна осуществляться с соблюдением требований действующего законодательства Российской Федерации, а также международно-правовых актом.

## 11. Контроль эффективности системы защиты

Контроль эффективности защиты персональных данных осуществляется с целью своевременного выявления и предотвращения нарушения целостности, доступности и конфиденциальности ПДн. Контроль может проводиться привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты персональных данных проводится с использованием технических и программных средств контроля, а также путем оценки реализованных в Обществе организационных и физических мер по защите ПДн.

## 12. Приложения

Приложение 1. Резюме Политики АО «ОХК «УРАЛХИМ» в отношении обработки персональных данных.

## Приложение 1. Резюме Политики АО «ОХК «УРАЛХИМ» в отношении обработки персональных данных

### Назначение документа

Политика определяет позицию и намерения Общества в области обработки и защиты персональных данных (ПДн) субъектов ПДн – лиц, состоящих в трудовых, гражданско-правовых и иных отношениях с Обществом (оператором ПДн).

Обработка и защита ПДн в Обществе осуществляется в полном соответствии с законодательством Российской Федерации с целью соблюдения законных прав субъектов ПДн на неприкосновенность частной жизни, личную и семейную тайну, а также с целью защиты интересов Общества от нанесения ущерба посредством нецелевого использования или воздействия на ПДн.

К ПДн относятся ФИО, дата и место рождения, адрес, сведения о семейном, социальном, имущественном положении, сведения об образовании, профессии, доходах и другая информация о субъекте ПДн.

### Обработка ПДн

Обработка ПДн включает сбор, получение, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение ПДн.

Обработка ПДн в Обществе осуществляется как с использованием средств автоматизации, так и без использования таких средств.

При обработке ПДн Общество придерживается следующих принципов:

- определяет цели обработки ПДн до начала обработки;
- собирает только необходимые и достаточные для заявленных целей ПДн;
- не собирает и не обрабатывает ПДн, касающиеся расовой и национальной принадлежности, политических, религиозных, философских и иных убеждений, состояния здоровья, интимной жизни, членства в общественных объединениях, в том числе профессиональных союзах;
- не раскрывает третьим лицам и не распространяет ПДн без согласия субъекта (за исключением случаев, предусмотренных законодательством Российской Федерации);
- уничтожает или обезличивает ПДн по достижении целей обработки или в случае утраты необходимости в достижении целей.

### Защита ПДн

Защита ПДн предполагает обеспечение и постоянное поддержание требуемых свойств ПДн – конфиденциальности, целостности и достоверности, доступности для целевого использования, защищенности от незаконного распространения.

Объектами системы безопасности ПДн Общества являются:

- информационная система персональных данных (ИСПДн) – совокупность содержащих ПДн баз данных, а также программных и аппаратных средств, обеспечивающих обработку и защиту ПДн;
- процессы обработки ПДн, регламенты и процедуры;
- объекты и помещения, в которых расположены компоненты ИСПДн.

Общество реализует комплекс правовых, организационных, технических и физических мер защиты ПДн, в том числе:

- регламентацию правил обработки ПДн с установлением прав, обязанностей и ответственности участников;
- подготовку ответственных за обеспечение безопасности ПДн;
- регламентацию допуска работников к ПДн;
- использование средств аутентификации и идентификации пользователей, а также средств разграничения прав доступа в ИСПДн;

- использование средств антивирусной защиты, резервного копирования и восстановления программных средств ИСПДН;
- создание механизма выявления и оперативного реагирования на угрозы безопасности ПДн;
- регламентацию процессов обслуживания и модификации программных и аппаратных средств ИСПДн;
- использование средств оперативного контроля и регистрации событий безопасности в ИСПДн;
- контроль неизменности конфигурации аппаратных средств ИСПДн;
- создание физических препятствий на путях доступа потенциальных нарушителей к ПДн с использованием электронно-механических устройств и сооружений, средств визуального наблюдения, связи и охранной сигнализации.