

Приложение № 1

УТВЕРЖДЕНО

приказом Генерального директора

АО «Ижевский мотозавод «Аксион-холдинг»

от «\_\_\_» \_\_\_\_\_ 2021 № \_\_\_\_\_

**ПОЛОЖЕНИЕ**  
**о защите персональных данных,**  
**обрабатываемых на средствах вычислительной техники**  
**в АО «Ижевский мотозавод «Аксион-холдинг»**

г. Ижевск 2021

## СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ.....	3
2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ.....	5
3. ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	7
4. ПОРЯДОК ОПРЕДЕЛЕНИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ.....	8
5. ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	9
6. ФУНКЦИИ ДОЛЖНОСТНЫХ ЛИЦ И ПОДРАЗДЕЛЕНИЙ.....	10
7. КОНТРОЛЬ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	11
8. ОТВЕТСТВЕННОСТЬ.....	12

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящее Положение определяет общие принципы организации работ по обеспечению безопасности персональных данных при их обработке на средствах вычислительной техники в АО «Ижевский мотозавод «Аксион-холдинг» (далее - Предприятие).

1.2 Настоящее Положение разработано в соответствии со следующими нормативными документами:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 14.02.2008;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 15.02.2008 (далее – Базовая модель угроз);
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3 Требования настоящего Положения обязательны для выполнения всеми работниками Предприятия.

1.4 Принимаемые меры по защите персональных данных на объектах информатизации Предприятия должны обеспечивать выполнение действующих требований и норм по защите информации.

Они должны быть технически выполнимы, экономически обоснованы, обеспечивать заданный уровень защиты.

Меры по защите персональных данных могут уточняться и дополняться по мере их реализации и совершенствования нормативно-правовой базы Российской Федерации в области защиты информации.

1.5 Контроль выполнения требований настоящего Положения возлагается на Заместителя генерального директора по вопросам защиты информации, режиму и безопасности.

## 2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

### 2.1 Принятые сокращения

ИС	-	информационная система
ИСПДн	-	информационная система персональных данных
НСД	-	несанкционированный доступ
ПДИТР и ТЗИ	-	противодействие иностранным техническим разведкам и техническая защита информации
ПДн	-	персональные данные
ПЭМИН	-	побочные электромагнитные излучения и наводки
ФСТЭК	-	Федеральная служба по техническому и экспортному контролю.

### 2.2 Термины и определения.

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

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

**Несанкционированный доступ** – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциям, предназначению и техническим характеристикам .

**Обработка персональных данных** – любое действие (операция) или совокупность действий, 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.

**Объект информатизации** – применительно к настоящему Положению: рабочее место, на котором производится обработка персональных данных, персональный компьютер, с которого ведётся обработка персональных данных, помещение,

предназначенное для работы с документами, содержащими персональные данные, и хранения носителей персональных данных.

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

***Субъект персональных данных*** – физическое лицо, прямо или косвенно определяемое на основании относящейся к нему информации.

### **3. ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

3.1 Целями защиты ПДн на Предприятии являются:

- предотвращение утечки ПДн по техническим каналам;
- предотвращение уничтожения, искажения, копирования, блокирования информации в ИСПДн за счёт НСД к ней;
- соблюдение законодательства РФ, конституционных прав и свобод субъектов персональных данных;
- сохранение возможности управления процессом обработки и пользования информацией.

3.2 К основным задачам защиты ПДн на Предприятии относятся:

- предотвращение передачи, разглашения ПДн лицам, не имеющим прав доступа к ПДн;
- предотвращение получения ПДн заинтересованным лицом с нарушением установленных прав и правил доступа к ПДн;
- предотвращение получения ПДн с помощью технических средств;
- предотвращение воздействия на ПДн с нарушением установленных прав и правил доступа, в результате чего происходит искажение, уничтожение, блокирование доступа к ПДн, а также утрата, уничтожение или сбой функционирования носителя ПДн;
- предотвращение воздействия на ПДн в результате ошибочных действий пользователя, сбоя технических и программных средств ИСПДн, природных явлений и иных нецеленаправленных на изменение ПДн мероприятий.

## **4. ПОРЯДОК ОПРЕДЕЛЕНИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ**

4.1 К защищаемой информации при обработке ПДн на Предприятии относится:

- информация, составляющая персональные данные работников Предприятия;
- информация, составляющая персональные данные соискателей на вакантные должности;
- информация, составляющая персональные данные близких родственников работников Предприятия и соискателей на вакантные должности (при оформлении допуска к сведениям, составляющим государственную тайну);
- информация о системе и средствах защиты ПДн;
- иная информация, составляющая ПДн, получаемая в рамках российского законодательства.

4.2 Объектами защиты при обработке ПДн являются:

- серверы корпоративной сети, на которых происходит обработка и хранение ПДн;
- персональные компьютеры, участвующие в обработке ПДн;
- все виды носителей, содержащих ПДн;
- каналы информационного обмена, по которым происходит передача ПДн.

4.3 На Предприятии разрабатываются Положение о персональных данных и Перечень ПДн.



## 5. ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 Постановку общих принципов работы и принятие наиболее важных решений по вопросам обеспечения защиты ПДн осуществляет Генеральный директор.

5.2 Для достижения поставленных целей и задач по защите ПДн на Предприятии проводятся следующие мероприятия:

- охрана территории;
- определение Перечня персональных данных, подлежащих защите;
- определение лиц, допущенных к обработке ПДн;
- классификация ИСПДн;
- составление Частной модели угроз и определение актуальных угроз безопасности ПДн;
- создание системы защиты ПДн при модернизации ИСПДн;
- составление организационно-распорядительной, проектной, эксплуатационной и иной документации по защите ПДн;
- защита информации, содержащей ПДн при их автоматизированной обработке, передаче с использованием технических средств, а также на документах и иных носителях;
- защита ПДн при работе в информационных сетях связи общего пользования;
- периодическое обучение работников правилам работы с ПДн;
- контроль выполнения мероприятий по обеспечению безопасности ПДн.

5.3 Перечень необходимых мер защиты ПДн определяется по результатам обследования всех объектов информатизации с учетом соотношения затрат на защиту ПДн, с учетом возможного ущерба субъекту ПДн от разглашения, уничтожения, искажения ПДн, а также с учетом реальных возможностей перехвата и раскрытия ПДн. Особое внимание должно быть уделено защите ПДн, в отношении которых угрозы реальны и сравнительно просто реализуемы без применения сложных технических средств перехвата ПДн.

5.4 Организационные и технические мероприятия по защите ПДн должны проводиться на всех этапах обработки ПДн.

5.5 Для выполнения работ по защите ПДн на Предприятии, отделом № 101 разрабатывается график проверок.

## **6. ФУНКЦИИ ДОЛЖНОСТНЫХ ЛИЦ И ПОДРАЗДЕЛЕНИЙ**

6.1 Бюро ПД ИТР и ТЗИ отдела № 101 осуществляет непосредственное руководство разработкой мероприятий по защите ПДн и контролю состояния защищенности ПДн обрабатываемых на средствах вычислительной техники на Предприятии.

6.2 Отдел № 136 обеспечивает надлежащее функционирование ИСПДн Предприятия, непосредственную реализацию мероприятий по защите ПДн в корпоративной сети Предприятия и принимает меры для предотвращения НСД.

6.3 Руководители структурных подразделений осуществляют мероприятия по соблюдению режима обработки персональных данных, циркулирующих на объектах информатизации подчиненных им подразделений, обеспечивают ознакомление работников подразделений с организационно-распорядительными документами Предприятия по защите ПДн.

6.4 Работники, осуществляющие обработку ПДн, обеспечивают выполнение установленных требований и норм по защите ПДн на своих рабочих местах.

## **7. КОНТРОЛЬ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

7.1 С целью проверки правильности функционирования системы защиты ПДн, выявления и предупреждения НСД работниками ПД ИТР и ТЗИ отдела № 101 с привлечением работников отдела № 136 проводится контроль защищенности ПДн, обрабатываемых на средствах вычислительной техники.

7.2 Контроль бывает плановым и внеплановым. Все работники Предприятия должны оказывать содействие в процессе осуществления контроля.

7.3 Основанием для проведения планового контроля является План проверок, утвержденный Заместителем Генерального директора по вопросам защиты информации, режиму и безопасности, а для внепланового контроля - его предписание.

7.4 По результатам проведенного контроля оформляется Акт, в котором отражаются состояние дел в области выполнения установленного порядка обращения с ПДн, выявленные недостатки и нарушения, а также вносятся предложения по их устранению. Акт составляется в двух экземплярах, подписывается проверяющими, руководителем структурного подразделения и утверждается Заместителем Генерального директора по вопросам защиты информации, режиму и безопасности. Один экземпляр Акта направляется в структурное подразделение, в котором проводилась проверка, другой — в бюро ПД ИТР и ТЗИ отдела № 101.

7.5 Рабочая группа может ходатайствовать перед руководством Предприятия о привлечении к ответственности лиц, виновных в нарушении требований по обеспечению безопасности ПДн.

## 8. ОТВЕТСТВЕННОСТЬ

8.1 Ответственность за общее состояние и организацию работ по обеспечению безопасности ПДн возлагается на руководство Предприятия: Генерального директора, Заместителя генерального директора по вопросам защиты информации, режиму и безопасности и Заместителя директора по персоналу, организационным социальным вопросам и информации.

8.2. Ответственность за организацию обработки ПДн возлагается на руководителей структурных подразделений.

8.3 Ответственность за непосредственную разработку мероприятий по защите ПДн, обрабатываемых на средствах вычислительной техники, возлагается на руководителя бюро ПД ИТР и ТЗИ отдела № 101.

8.4 Ответственность за непосредственную реализацию мероприятий по защите ПДн в корпоративной сети Предприятия и надлежащее функционирование ИСПДн Предприятия возлагается на Заместителя Генерального директора по информационным технологиям – начальника информационно-вычислительного центра.

8.5 Ответственность за обеспечение требований по защите ПДн, обрабатываемых в структурном подразделении, возлагается на руководителей структурных подразделений Предприятия, эксплуатирующих данные объекты.

8.6 Каждый работник Предприятия несет ответственность за свои действия с ПДн и в ИСПДн, предусмотренную действующим законодательством РФ и организационно-распорядительными документами Предприятия.

Начальник отдела № 101

Д.А. Андреев