Утверждена приказом
Публичного акционерного
общества
«Хадыженский машиностроительный
завод»
от «10» января 2018г.

Положение
об обеспечении безопасности персональных данных при их обработке в ПАО «ХМЗ»

1. Общие положения

1.1. Настоящее Положение об обеспечении безопасности персональных данных при их обработке в ПАО «ХМЗ» (далее – Положение) определяет меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

1.2. Целью настоящего Положения является обеспечение защиты прав граждан при обработке их персональных данных в информационных системах персональных данных при ведении кадровой работы на предприятии.

1.3. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 17.11.2007 г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и иными нормативно-правовыми актами.

1.4. Настоящее Положение вступает в силу с момента его утверждения генеральным директором ПАО «ХМЗ» и действует бессрочно до замены его новым Положением. Все изменения в настоящее Положение вносятся приказом ПАО «ХМЗ»

2. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.

2.1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры и обеспечивать их принятие для защиты 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.

2.2. Обеспечение безопасности персональных данных достигается, в частности:

2.2.1. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

2.2.2 Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных.

2.2.3. Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

2.2.4. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

2.2.5. Учетом машинных носителей персональных данных.

2.2.6. Обнаружение фактов несанкционировнного доступа к персональным данным и принятием мер.

2.2.7. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.2.8. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

2.2.9. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3.1. Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение,

блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

3.2. Определение угроз безопасности персональных данных осуществляется в модели угроз безопасности персональных данных соответствии с Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России от 15.02.2008 г.

4. Информационные системы персональных данных.

4.1. На предприятии используются следующие информационные системы персональных данных:

Наименование системы	Подразделения предприятия	Тип БД	Объем данных
1С Предприятие 8.3	БФО	Многопользовательская, SQL server	➢ 1000
	ОК		
	ОМ		
	ПЭО		
	ОМТС		

4.2. Используемые информационные системы персональных данных классифицированы по классу К3 в соответствии с Приказом ФСТЭК, ФСБ, Мининформсвязи России от 13.02.08 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

4.3. Классификация информационных систем персональных данных проведена по результатам анализа следующих исходных данных:

1) Категория обрабатываемых в информационной системе персональных данных: (в информационной системе 1С «Предприятие») - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
2) Объем персональных данных, обрабатываемых в системе: более 1000 субъектов персональных данных в информационной системе 1С «Предприятие
3) По заданным оператором характеристикам безопасности персональных данных информационные системы персональных данных предприятия являются типовыми информационными системами, требующими обеспечения конфиденциальности персональных данных.

4) По структуре информационные системы персональных данных являются комплексами автоматизированных рабочих мест, объединенными в единую информационную систему средствами связи без использования технологии удаленного доступа, т.е. являются локальными.
5) По наличию подключения к сетям общего пользования информационные системы персональных данных предприятия относятся к системам, имеющим подключения.
6) По режиму обработки персональных данных информационные системы персональных данных предприятия относятся к многопользовательским системам.
7) По разграничению прав доступа пользователей информационные системы персональных данных предприятия относится к системам с разграничением прав доступа.
8) Информационные системы персональных данных предприятия являются системами, все технические средства которых находятся в пределах Российской Федерации.

4.4. Класс информационной системы может быть пересмотрен: по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы; по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

4.5. Ответственным за безопасность персональных данных при обработке их на каждом отдельном АРМ является работник, осуществляющий обработку персональных данных с использованием этого АРМ.

6. Перечень персональных данных, обрабатываемых в информационных системах персональных данных

6.1. В информационных системах персональных данных предприятия обрабатываются следующие персональные данные субъектов, не являющихся работниками предприятия, позволяющие идентифицировать данного субъекта персональных данных:

- Фамилия, имя отчество;
- Дата рождения;
- Контактный телефон;
- Адрес регистрации или фактического проживания;
- Паспортные данные.

6.2. В информационной системе персональных данных 1С «Зарплата и кадры» помимо персональных данных, позволяющих идентифицировать

работника предприятия, могут обрабатываться прочие персональные данные работников предприятия:

- Информация об образовании;
- Информация о трудовой деятельности;
- Информация о трудовом стаже;
- Семейное положение и состав семьи;
- Информация о знании иностранных языков;
- Информация о заработной плате;
- Данные о трудовом договоре;
- Сведения о воинском учете;
- ИНН;
- Данные о повышении квалификации и аттестации, о наградах, медалях и поощрениях;
- Информация о приеме на работу, перемещении по должности, увольнениях, выходах в отпуск;
- Информация о пенсионном обеспечении

и прочие персональные данные, за исключением персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

7. Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

7.1. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

7.2. Уровень требований, предъявляемых по обеспечению безопасности персональных данных, обрабатываемых в информационных системах предприятия, зависит от состава актуальных угроз и класса информационной системы персональных данных. Для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных класса 3 система защиты персональных данных должна включать:

- управление доступом;
- регистрацию и учет;
- обеспечение целостности персональных данных;
- криптографическую защиту;

- антивирусную защиту;
- предотвращение и обнаружение вторжений.

7.3. Система управления доступом реализована в информационных системах персональных данных предприятия и позволяет разграничивать доступ пользователей к отдельным объектам системы и отдельным группам персональных данных.

7.3.1. Пользователи информационных систем персональных данных объединены в группы, обладающие определенными ролями в процессе обработки данных. Роли определяют, какими правами доступа обладают пользователи информационных систем персональных данных.

7.3.2. Аутентификация пользователя при доступе к информационным системам персональных данных осуществляется с помощью уникального идентификатора пользователя (логина) и пароля.
7.3.2.1. Ответственным за неразглашение пароля назначается пользователь информационной системы персональных данных.

7.3.2.2. В случае, если создалась угроза компрометации пароля пользователя информационных систем персональных данных, пользователь обязан незамедлительно обратиться к программистам предприятия, ответственным за безопасность персональных данных при их автоматизированной обработке, для внеплановой смены пароля.

7.3.3. Физический доступ посторонних лиц к рабочим местам пользователей информационных систем персональных данных запрещен. Персональные данные обрабатываются в отдельных помещениях, а пользовательские терминалы имеют функцию автоблокировки по истечению заданного времени бездействия.

7.3.4. Хранение централизованных баз данных информационных систем персональных данных осуществляется на основных серверах предприятия, расположенных в специально выделенном, закрытом помещении (серверной) со строго ограниченным доступом. Доступ в серверную имеют только программисты предприятия, ответственные за безопасность персональных данных при их автоматизированной обработке. Сетевой доступ к базам данных информационных систем персональных данных разграничен по правам доступа ролей пользователей, ведущих обработку персональных данных.

7.3.5. Доступ в глобальную сеть Интернет на рабочих местах пользователей информационных систем персональных данных запрещен на уровне настроек автоматизированного рабочего места, а также на уровне прокси-сервера предприятия, осуществляющего централизованный доступ в Интернет.

Использование GSM-модемов на рабочих местах пользователей информационных систем персональных данных запрещено.

7.4. Система регистрации и учета реализована в информационных системах персональных данных предприятия в виде электронных журналов учета действий пользователя, в которых регистрируются подлежащие учету действия пользователя: дата и время доступа пользователя к информационной системе персональных данных, тип объекта информационной системы, к которому был осуществлен доступ, вид действия, которое было произведено с объектом информационной системы.

7.5. Обеспечение целостности персональных данных при обработке в информационных системах персональных данных достигается применением процедуры автоматического многократно дублированного резервного копирования персональных данных с возможностью их быстрого восстановления в случае их изменения, повреждения, блокирования или уничтожения в следствие технологической аварии или несанкционированного доступа.

7.5.1. Резервные копии персональных данных дублируются на основных серверах предприятия, а также на компьютере программиста предприятия, ответственного за резервное копирование персональных данных. Резервные копии персональных данных хранятся в виде электронных архивов в течение длительного времени, что позволяет в случае необходимости восстановить их с разной степенью актуальности. Файловый и сетевой доступ к резервным копиям персональных данных ограничен программистами предприятия, ответственными за резервное копирование и безопасность персональных данных при их автоматизированной обработке.

7.5.3. Программист предприятия, ответственный за резервное копирование персональных данных, может в течение рабочего дня создавать резервные копии персональных данных по своему усмотрению в целях предотвращения их изменения, повреждения или уничтожения.

7.5.4. Резервные копии персональных данных могут быть записаны на твердотельные диски (DVD-ROM) для долговременного хранения. Запись резервной копии персональных данных на твердотельный диск осуществляется программистом предприятия, ответственным за резервное копирование персональных данных. Факт записи фиксируется в «Журнале учета записей резервных копий персональных данных для долговременного хранения». Резервные копии персональных данных на твердотельных дисках хранятся в специально оборудованном, закрытом помещении с ограниченным доступом.

7.6. Криптографическая защита персональных данных в информационных системах персональных данных предприятия применяется в случае передачи персональных данных по сетям общего пользования для обработки в сторонние организации, с которыми заключены соответствующие договоры. Криптографическая защита персональных данных основана на применении электронно-цифровой подписи и сертифицированного криптографического комплекса КриптоПро.

7.7. Антивирусная защита персональных данных обеспечена применением антивирусного программного комплекса на всех компьютерах предприятия. Обновление антивирусных баз осуществляется ежедневно автоматически под контролем программиста предприятия, ответственного за антивирусную защиту.

7.8. Предотвращение вторжений в электронно-вычислительную сеть предприятия и информационные системы персональных данных обеспечено следующими мерами:

- разграничение доступа пользователей к компьютерам с использованием логина и пароля;
- разграничение доступа пользователей к объектам информационных систем согласно ролям пользователей;
- автоматическая блокировка неиспользуемых длительное время терминалов;
- использование специально оборудованного, закрытого помещения с ограниченным доступом для содержания центральных серверов предприятия и хранения резервных копий персональных и технологических данных;
- использование брандмауэров на персональных компьютерах пользователей и серверах предприятия;
- исключение непосредственного доступа в глобальную сеть Интернет рабочих мест, на которых ведется обработка персональных данных, и серверов предприятия;
- применение криптографической защиты в сеансе обмена данными через глобальную сеть Интернет в тех случаях, когда это необходимо для передачи персональных данных;
- использование централизованного прокси-сервера, брандмауэра и технологии трансляции сетевых адресов (NAT) для разграничения и контроля доступа пользователей в Интернет, не ведущих непосредственную обработку персональных данных, а также предотвращения непосредственного доступа из сети Интернет в локально-вычислительную сеть предприятия;
- использование брандмауэра и технологии трансляции сетевых адресов (NAT) для организации доступа пользователей глобальной сети Интернет к веб-серверу предприятия (сервер скрыт внутри сети от несанкционированного доступа);

- регулярный мониторинг уязвимостей используемого программного обеспечения программистами предприятия, ответственными за безопасность персональных данных при их автоматизированной обработке, и обновление его в случае обнаружения критических уязвимостей;
- регулярное резервное копирование системной технологической информации: файлов конфигурации, журналов регистрации, базы данных контроллеров домена, веб-сервера предприятия и прочей технологической информации.

Для обнаружения вторжений программистами предприятия, ответственными за безопасность персональных данных при их автоматизированной обработке, проводится регулярный анализ файлов регистрации прокси-сервера, веб-сервера и основных серверов предприятия.

8. Осуществление контроля за принимаемыми мерами по обеспечению безопасности персональных данных

8.1. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных при обработке их в информационных системах персональных данных предприятия осуществляют программисты предприятия, ответственные за безопасность персональных данных при их автоматизированной обработке.

8.2. Программисты предприятия, ответственные за безопасность персональных данных при их автоматизированной обработке, обеспечивают:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным или же их изменения, повреждения, блокировки или уничтожения;
- осуществление режима разграничения доступа пользователей к информационным системам персональных данных;
- осуществление контроля за плановой сменой паролей пользователей, осуществляющих обработку персональных данных;
- недопущение воздействий на технические средства автоматизированной оборабатки персональных данных, в результате которых может быть нарушено их функционирование;
- поддержание в работоспособном состоянии и своевременное обновление технических и программных средств авоматизированной обработки персональных данных;
- возможность незамедлительного восстановления персональных данных из резервных копий в случаях их изменения, повреждения, блокировки или

уничтожения вследствие технологических неисправностей или несанкционированного доступа;
- контроль за осуществлением регулярного резервного копирования персональных данных;
- формирование и поддержание в актуальном состоянии перечней информационных систем персональных данных и автоматизированных рабочих мест, используемых для обработки персональных данных, а также списков работников, ответственных за безопасность персональных данных при их обработке на конкретном автоматизированном рабочем месте;
- проведение инструктажа работников по безопасности персональных данных при обработке их на автоматизированных рабочих местах;
- прочий контроль за соблюдением мер, направленных на обеспечение защиты персональных данных при их обработке в информационных системах персональных данных.

9. Права и обязанности работников, осуществляющих обработку персональных данных на автоматизированных рабочих местах.

9.1. Работник, осуществляющий обработку персональных данных на автоматизированном рабочем месте, обязан:

- знать и выполнять требования действующих нормативных актов предприятия в сфере обработки персональных данных;
- знать и соблюдать установленные требования по условиям и порядку обработки персональных данных, учету, обеспечению безопасности персональных данных;
- соблюдать требования правил создания и использования паролей доступа к информационным системам персональных данных, в частности, обеспечивать: неразглашение своего индивидуального логина и пароля, в том числе в письменном виде в качестве записок-напоминаний, пометок и т.п, своевременную плановую смену пароля или внеплановую в случае угрозы его разглашения;
- обеспечивать недопущение за свое рабочее место посторонних лиц, а также работников, не имеющих доступ к обработке персональных данных на его рабочем месте;
- экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами, жалюзи на оконных проемах должны быть закрыты;
- блокировать терминал своего рабочего места при его покидании путем нажатия комбинации Win+L на клавиатуре либо комбинации Ctrl+Alt+Del и выбора опции «Блокировать компьютер»;
- незамедлительно извещать программистов предприятия, ответственных за безопасность персональных данных при их автоматизированной обработке, в

случае выявленных фактов изменения, повреждения, блокирования или уничтожения персональных данных.

9.2. Работнику, осуществляющему обработку персональных данных на автоматизированном рабочем месте, запрещается:

- разглашать персональные данные третьим лицам;
- копировать персональные данные на внешние носители либо общедоступные сетевые ресурсы без разрешения своего непосредственного руководителя;
- самостоятельно вмешиваться в функционирование аппаратных и программных составляющих своего автоматизированного рабочего места, устанавливать программы, драйверы, GSM-модемы, подключать мобильные устройства и тому подобное оборудование;
- несанкционированно, без разрешения своего непосредственного руководителя и консультации с программистами предприятия, ответственными за безопасность персональных данных при их автоматизированной обработке, открывать общий доступ к папкам на своем автоматизированном рабочем месте;
- отключать или блокировать средства защиты информации такие, как антивирусная система и сетевой брандмауэр;
- хранить и обрабатывать на своем автоматизированном рабочем месте информацию личного характера и прочую информацию, не имеющую непосредственного отношения к должностным обязанностям работника;
- привлекать посторонних лиц для производства ремонта или настройки своего автоматизированного рабочего места.

9.3. Работник, осуществляющий обработку персональных данных на автоматизированном рабочем месте, имеет право получать инструктаж по безопасности персональных данных у программистов предприятия, ответственных за безопасность персональных данных при их автоматизированной обработке, а также обращаться к ним по иным вопросам в целях обеспечения безопасности персональных данных.