# Политика безопасности предприятия

# в отношении обработки персональных данных сотрудников предприятия и сотрудников контрагентов

# Введение

В Конституции Российской Федерации на высшем правовом уровне закреплено отношение государства к человеку «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина - обязанность государства».

Для выполнения своих обязанностей перед работниками предприятие (например, начисление и выплата заработной платы) вынуждено обрабатывать такие сведения как фамилия, имя отчество, место регистрации и т. д., которые носят название **персональных данных**. В общем случае под персональными данными (ПДн) Российское законодательство понимает **любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).**

Если предприятие предоставляет услуги на договорной основе физическим лицам (клиентам), то оно также обязано обрабатывать персональные данные клиентов.

Современное производство (любой бизнес) требует многочисленных информационных взаимоотношений с другими предприятиями для реализации разделения труда, а также с государственными и муниципальными структурами для отчетности и других функций. В этот информационный обмен включены среди прочих также **персональные данные работников предприятия, работников контрагентов, клиентов предприятия.**

Общие требования к защите персональных данных, обрабатываемых в информационных системах персональных данных (ИСПДн), изложены в:

1. Федеральном Законе от 27 июля 2006 года №152-ФЗ *«О персональных данных»*,
2. Постановлении правительства от 1 ноября 2012 г. № 1119 *«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»*,
3. Постановление правительства Российской Федерации от 21 марта 2012 г. № 211 «*Об утверждении перечня мер, направленных на обеспечение выполнение обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными и правовыми актами, операторами, являющимися государственными или муниципальными органами»*
4. В приказе Федеральной Службы по Техническому и Экспортному контролю (ФСТЭК) от 18 февраля 2013 г. № 21 *«Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»*,
5. В приказе Федеральной службы РФ (ФСБ) № 378 от 10 июля 2014 г. *«Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»*.

Контроль над исполнением организационных требований по защите ПДн возложен на Федеральную службу по надзору в сфере связи, информационных технологий, и массовых коммуникаций (РосКомНадзор), сайт Управления Роскомнадзора по Владимирской области <http://33.rkn.gov.ru>.

Контроль над исполнением технических требований по защите ПДн возложен на Федеральную службу по техническому и экспортному контролю (ФСТЭК).

Управления ФСТЭК расположены в федеральных округах, сайт <http://www.fstec.ru> .

Контроль над исполнением технических требований по защите ПДн с использованием криптографических средств возложен на Федеральную службу безопасности (ФСБ). Управления и отделы ФСБ расположены в отдельных регионах и субъектах РФ, сайт <http://fsb.ru>.

Высшее руководство предприятия, всемерно признавая конституционные права граждан Российской Федерации и понимая, что благосостояние работодателя, сотрудников, контрагентов и клиентов всецело зависит от их гармоничного общего взаимодействия, прикладывает все необходимые усилия для адекватной защиты персональных данных и поддерживающей инфраструктуры информационных систем.

# Цель политики безопасности

Цель политики безопасности обеспечить условия (финансовое обеспечение, правовое обеспечение, организационное обеспечение, техническое обеспечение) для требуемого законодательством уровня безопасности персональных данных, переданных субъектами персональных данных предприятию для обработки, а именно:

* Конфиденциальность (запрет на несанкционированный доступ к данным);
* Целостность (устойчивость ПДн к несанкционированному изменению, актуальность и непротиворечивость ПДн);
* Доступность (возможность обработки ПДн в штатном режиме, возможность за приемлемое время получить требуемую информационную услугу);
* Неотрекаемость (возможность доказать авторство информационного сообщения).

# Меры, принятые на предприятии по обеспечению безопасности ПДн

# Приказом по орагниации назначены ответственные за организацию обработки и защиты персональных данных (администратор безопасности);

# Определен перечень и объем и категории ПДн;

# Разработаны и приняты положение об обработке ПДн и другие необходимые документы пакета организационно-распорядительной документации;

# Лица, допущенные к обработке ПДн, обучены, ознакомлены под роспись с требованиями безопасности при обработке в ИСПДн;

# Определены уровни защищенности ПДн и актуальные угрозы безопасности;

# Технические средства, задействованные в информационных системах персональных данных Финансового управления администрации муниципального образования Юрьев-Польский район находятся в помещениях Финансового управления администрации муниципального образования Юрьев-Польский район.

# Ограничен физический доступ в помещения, где размещены технические средства ИСПДн;

# Используется дискреционный метод управления разграничением доступа к ПДн, реализованный в подсистеме идентификации, аутентификации и авторизации пользователей ПДн;

# Организована систематическая архивация персональных данных, позволяющая восстановить их после деструктивных воздействий естественного или искусственного характера.

# На каждом компьютере установлен агент антивирусной сети с централизованным управлением, сертифицированный ФСТЭК;

# Машинные носители учитываются в журналах учета машинных носителей;

# Персональные данные и носители персональных данных, используемые в информационных системах персональных данных и выводимые из обращения, уничтожаются в соответствии с порядком, определенным в Положении «Об обработке персональных данных».

# В соответствии с планом внутренних проверок осуществляется периодический контроль актуальности организационно-распорядительной документации, контроль работоспособности технических средств защиты путем тестирования на проникновение, контроль безопасности процедур, выполняемых пользователями информационных систем.