УТВЕРЖДЕНЫ

постановлением администрации

Ныровского сельского поселения

от 21.04.2014 № 51

**ПРАВИЛА**

**осуществления внутреннего контроля**

**соответствия обработки персональных данных  
требованиям к защите персональных данных, установленных федеральным законом «о персональных данных»,**

**принятыми в соответствии с ним нормативными   
 правовыми актами и локальными актами**

**1. Общие положения**

1. Настоящим документом «Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами» (далее – Правила) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.
2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2007 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и другими нормативными правовыми актами, ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
3. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152 ФЗ «О персональных данных».
4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в администрации Ныровского сельского поселения (далее – администрация) организовывается проведение периодических проверок условий обработки персональных данных.
5. Проверки осуществляются ответственным за организацию обработки персональных данных в администрации или комиссией, образуемой постановлением администрации Ныровского сельского поселения.

В проведении проверки не может участвовать сотрудник администрации, прямо или косвенно заинтересованный в её результатах.

1. Проверки соответствия обработки персональных данных установленным требованиям в администрации проводятся на основании утвержденного администрацией ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в учреждение письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется по указанию администрации в течение трех рабочих дней с момента поступления соответствующего заявления.
2. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

* порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
* порядок и условия применения средств защиты информации;
* эффективность принимаемых мер по обеспечению безопасности персональных данных;
* состояние учета электронных носителей персональных данных;
* соблюдение правил доступа к персональным данным;
* наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
* мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
* осуществление мероприятий по обеспечению целостности персональных данных.

кономичны, чем на корректирующие действия.

1.8.   В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в администрации (членам комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

1.9Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении (плановой даты начала проверки). О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, главе администрации докладывает ответственный за организацию обработки персональных данных либо председатель комиссии, в форме письменного заключения.

1.10  Контроль за своевременностью и правильностью проведения внеплановой проверки осуществляет должностное лицо, её назначившее.

2. **Планирование мероприятий внутреннего контроля**

2.1  Мероприятия по внутреннему контролю планируются ежегодно. Мероприятия планируются на один год должностным лицом, ответственным за организацию обработки персональных данных. Типовой план приведён в приложении №1 к настоящему Положению. Если предполагаемые к проведению мероприятия отличаются от приведённых в приложении №1, то составляется отдельный план на год. Содержание мероприятий по внутреннему контролю и сроки их проведения доводятся до всех лиц, в них участвующих (как проверяющих, так и проверяемых).

3. **Осуществление мероприятий внутреннего контроля**

3.1 Все мероприятия внутреннего контроля фиксируются в Журнале учета мероприятий внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора» (приложение №2). В этом журнале фиксируются также внеплановые мероприятия и инциденты, связанные с безопасностью персональных данных. Если по результатам мероприятия составляется отчётный либо иной документ (например, служебная записка), то указывается его наименование и регистрационный номер (при наличии).

3.2 Под инцидентом понимается любое непредвиденное или нежелательное событие, которое может нарушить безопасность персональных данных. Инцидентами являются:

* утрата услуг, оборудования, устройств;
* системные сбои или перегрузки;
* ошибки пользователей;
* несоблюдение локальных актов (политики, положений, инструкций);
* сбои программного обеспечения и отказы технических средств;
* нарушение правил доступа.

3.3 Сотрудник, выявивший несоответствие обработки персональных данных, технические уязвимости или инциденты, обязан немедленно сообщить ответственному за организацию обработки персональных данных через своего непосредственного начальника или администратора безопасности. Ответственный за организацию обработки персональных данных обязан организовать принятие соответствующих мер по устранению риска, связанного с несоответствием, уязвимостью, обеспечить быстрое, эффективное и последовательное реагирование.

3.4 На случай, если несоответствие, инцидент безопасности может привести к судебному разбирательству (гражданскому или уголовному) против должностного лица или администрации, информация должна быть собрана, сохранена и представлена согласно правилам оформления доказательств.

3.5 В обоснованных случаях реагирование на несоответствие, инцидент безопасности может включать инструктаж персонала по мерам безопасности персональных данных. Результаты инструктажа фиксируются в Журнале инструктажа по мерам безопасности персональных данных. Форма Журнала приведена в приложении №3.

3.6 В целях сокращения времени реагирования на инцидент безопасности инструктаж сотрудников может предваряться рассылкой информационных сообщений об инциденте безопасности с указанием мер (корректирующего и упреждающего характера) по недопущению подобных инцидентов. Рассылка пользователям ИСПДн информационных сообщений по вопросам информационной безопасности может использоваться и как профилактическая мера, не связанная с фактами инцидентов безопасности в учреждении. Рассылка информационных сообщений регистрируется в разделе I Журнала инструктажа по мерам безопасности персональных данных.

4. **Анализ результатов**

4.1  Анализ результатов внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами проводится в соответствии с утверждённым планом, с периодичностью не реже 1 раза в год, в целях обеспечения их пригодности, адекватности и результативности. В случае серьёзных или повторяющихся инцидентов анализ может проводиться и вне плана. Результаты анализа должны содержать предложения по совершенствованию принимаемых мер. По результатам анализа оформляется итоговый документ, который учитывается в Журнале учета мероприятий по контролю соответствия обработки персональных данных требованиям к защите персональных данных (приложение №2).

4.2  Входными данными для анализа являются:

* сведения, приведённые в итоговых документах предыдущих анализов;
* результаты взаимодействия с заинтересованными сторонами;
* методы, средства и процедуры, которые могут быть использованы для совершенствования принимаемых мер;
* правовое обоснование предупреждающих и корректирующих воздействий;
* уязвимости или угрозы, которые не были адекватно учтены в процессе оценки рисков;
* действия, совершённые по результатам предыдущего анализа;
* любые рекомендации по улучшению.

4.3  Выходные данные должны включать в себя все решения и действия, направленные на повышение эффективности принимаемых мер, на модификацию процедур и мер управления и контроля, с целью обеспечить реагирование на внутренние и внешние события безопасности персональных данных.

# 5. **Улучшение принимаемых мер по обеспечению соответствия обработки персональных данных требованиям к защите персональных данных**

5.1 Результаты анализа внутреннего контроля используются для выработки корректирующих и упреждающих действий.

К корректирующим действиям относятся мероприятия по выявлению несоответствий установленным требованиям, определению их причин, определению и реализации самих необходимых действий (корректировка планов и локальных актов, обновление технических и программных средств и средств защиты ИСПДн и т.п.).

К предупреждающим действиям относятся мероприятия по выявлению потенциальных несоответствий, определению их причин, определению и реализации самих необходимых действий (корректировка планов и локальных актов, обновление технических и программных средств и средств защиты ИСПДн и т.п.) Приоритеты в отношении предупреждающих действий определяются на основе оценки риска. Следует учитывать, что затраты на проведению мероприятий по предотвращению несоответствий более экономичны, чем на корректирующие действия.