

Муниципальное автономное общеобразовательное учреждение
Мальковская средняя общеобразовательная школа
Тюменская область, Тюменский район
ул. Совхозная 23, 625517 с. Мальково тел (факс) 776-038, 776-183

УТВЕРЖДАЮ

Директор школы

В.В.Зайцева

2015г.



**РЕГЛАМЕНТ
ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ
ЗА ОБЕСПЕЧЕНИЕМ УРОВНЯ ЗАЩИЩЕННОСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ И
СОБЛЮДЕНИЙ УСЛОВИЙ ИСПОЛЬЗОВАНИЯ СРЕДСТВ ЗАЩИТЫ
ИНФОРМАЦИИ, А ТАКЖЕ СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ
ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В
ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ
МАОУ МАЛЬКОВСКОЙ СОШ**

КОПИЯ
ДИРЕКТОР



СОДЕРЖАНИЕ

1 Общие положения	3
2 Порядок подготовки к проведению контрольных мероприятий.....	4
2.1 Виды контрольных мероприятий	4
2.2 План проведения контрольных мероприятий	4
2.3 Оформление результатов проведенных контрольных мероприятий	4
3 Общий порядок проведения контрольных мероприятий.....	6
3.1 Контрольные мероприятия в подсистеме управления доступом	6
3.2 Контрольные мероприятия в подсистеме регистрации и учета	6
3.3 Контрольные мероприятия в подсистеме обеспечения целостности	7
3.4 Контрольные мероприятия в подсистеме антивирусной защиты	7
3.5 Контрольные мероприятия в подсистеме обеспечения безопасного межсетевого взаимодействия	8
3.6 Контрольные мероприятия в подсистеме анализа защищенности	8
3.7 Контрольные мероприятия в подсистеме обнаружения и предотвращения вторжений	8
3.8 Контрольные мероприятия в подсистеме защиты от утечек по техническим каналам	8
3.9 Контрольные мероприятия в подсистеме физической защиты	8
3.10 Контрольные мероприятия в подсистеме криптографической защиты	9
Приложение 1. Журнал учета мероприятий по обеспечению и контролю безопасности ПДн, обрабатываемых в ИСПДн МАОУ Мальковской СОШ	10

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Регламент осуществления внутреннего контроля за обеспечением уровня защищенности персональных данных и соблюдения условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в информационных системах персональных данных МАОУ Мальковской СОШ (далее – Регламент) устанавливает и определяет единый и обязательный порядок проведения контрольных мероприятий для каждой из подсистем, входящих в систему защиты персональных данных информационных систем персональных данных (далее - ИСПДн) «Наименование организации» (далее - «МАОУ МАЛЬКОВСКОЙ СОШ»).

Настоящий Регламент утверждается и вводится в действие руководителем МАОУ Мальковской СОШ и является обязательным для исполнения.

2 ПОРЯДОК ПОДГОТОВКИ К ПРОВЕДЕНИЮ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн МАОУ МАЛЬКОВСКОЙ СОШ проводятся в следующих целях:

- проверка выполнения требований организационно-распорядительной документации «МАОУ МАЛЬКОВСКОЙ СОШ и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;
- оценка уровня осведомленности и знаний работников «МАОУ МАЛЬКОВСКОЙ СОШ в области обработки и защиты персональных данных (далее - ПДн);
- оценка обоснованности и эффективности применяемых мер и средств защиты.

2.1 Виды контрольных мероприятий

Контрольные мероприятия подразделяются на внутренние и внешние. Внутренние контрольные мероприятия осуществляются силами работников МАОУ Мальковской СОШ, ответственных за обеспечение безопасности ПДн. При проведении внешних контрольных мероприятий привлекаются сторонние организации.

Кроме того, контрольные мероприятия подразделяются на плановые и внеплановые.

Плановые контрольные мероприятия проводятся периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее - План) и направлены на постоянное совершенствование системы защиты персональных данных «МАОУ МАЛЬКОВСКОЙ СОШ.

Внеплановые контрольные мероприятия проводятся на основании решения инженера по безопасности группы информационных технологий. Решение о проведении внеплановых контрольных мероприятий может быть принято в следующих случаях:

- по результатам расследования инцидента информационной безопасности;
- по результатам внешних контрольных мероприятий, проводимых регулируемыми органами.

Кроме того любой работник «МАОУ МАЛЬКОВСКОЙ СОШ вправе подготавливать обоснованные предложения о необходимости проведения внеплановых контрольных мероприятий и предоставить их лицу, ответственному за обеспечение безопасности ПДн.

2.2 План проведения контрольных мероприятий

Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

План проведения внутренних контрольных мероприятий (как плановых, так и внеплановых) включает следующие сведения по каждому из мероприятий:

- цели проведения контрольных мероприятий;
- задачи проведения контрольных мероприятий,
- объекты контроля (процессы, подразделения, информационные системы и т.п.);
- состав участников, привлекаемых для проведения контрольных мероприятий;
- сроки и этапы проведения контрольных мероприятий.

Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий (см. раздел 2.3).

2.3 Оформление результатов проведенных контрольных мероприятий

По итогам проведения внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает отчет, в котором указывается:

- описание проведенных мероприятий по каждому из этапов в соответствии с планом;
- отклонения от плана, в случае их наличия;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений.
- заключение по итогам проведения внутреннего контрольного мероприятия.

Отчет передается на рассмотрение руководству «МАОУ МАЛЬКОВСКОЙ СОШ.

Общая информация о проведенном контрольном мероприятии фиксируется в Журнале учета мероприятий по обеспечению и контролю безопасности ПДн, обрабатываемых в ИСПДн МАОУ Мальковской СОШ (см. Приложение 1 настоящего Регламента).

3 ОБЩИЙ ПОРЯДОК ПРОВЕДЕНИЯ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

Контрольные мероприятия проводятся при обязательном участии лица, ответственному за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы информационных систем, администраторы информационной безопасности.

Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

3.1 Контрольные мероприятия в подсистеме управления доступом

При проведении контрольных мероприятий в подсистеме управления доступом, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия установленных прав доступа (в прикладных системах, базах данных и т.п.) полномочиям в рамках трудовых обязанностей работника;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка процесса идентификации, аутентификации и авторизации при входе пользователя в систему (обращении к информационным ресурсам информационных систем);
- проверка механизмов блокирования доступа к средствам защиты от несанкционированного доступа¹ (далее - НСД) при выполнении устанавливаемого числа неудачных попыток ввода пароля;
- проверка системы смены пароля принудительным образом (по истечению срока действия пароля);
- проверка выполнения требований по стойкости пароля.

3.2 Контрольные мероприятия в подсистеме регистрации и учета

При проведении контрольных мероприятий в подсистеме регистрации и учета, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка системных журналов на наличие зарегистрированных попыток несанкционированного доступа;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации и внутренних документах компании;
- имитация попытки несанкционированного доступа в систему, для проверки работы системы регистрации попытки НСД в системном журнале;
- проверка способов защиты системного журнала регистрации от уничтожения или модификации нарушителем²;
- проверка функционирующей системы автоматического непрерывного мониторинга событий в системе, которые могут являться причиной реализации угроз (создание, редактирование, запись, компиляция объектов).

Кроме того, при проведении проверок в части учета и хранения носителей персональных данных могут выполняться следующие проверки:

- проверка мест хранения носителей ПДн, сейфов и металлических шкафов, надежность их замков;
- проверка выполнения установленного порядка учета и хранения носителей ПДн;

¹ Несанкционированный доступ - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационной системой

² Нарушитель (субъект атаки) – лицо (или иницируемый им процесс), проводящее (проводящий) атаку.

- проверка фактического наличия всех носителей ПДн, в том числе учетные журналы, дела, документы (поступившие, изданные, переведенные на выделенное хранение);
- проверка фактического наличия всех носителей ПДн, переданных на архивное хранение;
- проверка фактического наличия всех не подшитых в дела и поступивших документов, содержащих ПДн, независимо от даты их регистрации;
- проверка номенклатуры дел с целью выделения документов, содержащих ПДн, для передачи в архив или на уничтожение;
- проверка правильности проставления регистрационных данных носителей, документов и дел, и учетных журналов;
- проверка правильности проставления в журнале отметок о движении носителей.

3.3 Контрольные мероприятия в подсистеме обеспечения целостности

При проведении контрольных мероприятий в подсистеме обеспечения целостности, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка механизмов контроля целостности пакетов обновлений средств защиты информации с использованием контрольных сумм;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка целостности используемого программного обеспечения, путем вычисления контрольных сумм;
- проверка фактического наличия экземпляров резервных копий;
- проверка целостности сделанных резервных копий путем восстановления данных;
- имитация выполнения резервного копирования и восстановления данных при аварийном режиме функционирования системы.

3.4 Контрольные мероприятия в подсистеме антивирусной защиты

При проведении контрольных мероприятий в подсистеме антивирусной защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка рабочих станций и серверов станций на наличие установленных программных средств антивирусной защиты;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка механизма своевременного обновления программных средств антивирусной защиты (в т.ч. баз данных вирусных сигнатур) на всех рабочих и серверных станциях;
- запуск полного сканирования системы в режиме реального времени антивирусным средством;
- проверка антивирусным средством используемых отчуждаемых носителей;
- проверка функционирования механизмов принудительной проверки используемых съемных носителей;
- имитация попыток заражения вредоносным программным обеспечением³ серверных и рабочих станций;
- просмотр системных журналов и отчетов на наличие зафиксированных случаев заражения вредоносным ПО.

³ Вредоносное программное обеспечение - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных

3.5 Контрольные мероприятия в подсистеме обеспечения безопасного межсетевого взаимодействия

При проведении контрольных мероприятий в подсистеме обеспечения безопасного межсетевого взаимодействия, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия установленных межсетевых экранов требуемому уровню защищенности;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- имитация попыток проникновения в «закрытый» сегмент сети из открытого, в том числе с применением специального ПО;
- проверка системных журналов на наличие зафиксированных попыток обращения к «закрытым» ресурсам.

3.6 Контрольные мероприятия в подсистеме анализа защищенности

При проведении контрольных мероприятий в подсистеме анализа защищенности, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка выполнения своевременного обновления ПО, используемого для анализа защищенности, в т.ч. баз данных уязвимостей;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- имитация попыток преодоления системы защиты, проверка системных журналов на наличие зафиксированных попыток НСД.

3.7 Контрольные мероприятия в подсистеме обнаружения и предотвращения вторжений

При проведении контрольных мероприятий в подсистеме обнаружения и предотвращения вторжений, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации.

3.8 Контрольные мероприятия в подсистеме защиты от утечек по техническим каналам

При проведении контрольных мероприятий в подсистеме защиты от утечек по техническим каналам, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка в помещениях, где ведется обработка ПДн, установленных на окна жалюзи, штор и т.п.;
- проверка размещения дисплеев рабочих станций, серверов и демонстрационного оборудования (проекторы, телевизоры и т.п.) таким образом, чтобы исключалась возможность просмотра посторонними лицами текстовой и графической информации, содержащей персональные данные.

3.9 Контрольные мероприятия в подсистеме физической защиты

При проведении контрольных мероприятий в подсистеме физической защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка введения журналов учета посетителей, проходящих на территорию «МАОУ МАЛЬКОВСКОЙ СОШ»;
- проверка введения журналов посетителей, проходящих в защищаемые помещения;
- проверка электронных журналов СКУД на предмет попыток НСД в защищаемые помещения сотрудников, не имеющих права доступа в данные помещения;
- проверка наличия ключей (в том числе и электронных пропусков) от защищаемых помещений, а так же проверка сохранности вторых экземпляров ключей от защищаемых помещений;

- просмотр всех заявлений об утерянных ключах (в том числе и электронных пропусках) по которым можно получить доступ в защищаемые помещения, а так же проверка принятых мер (блокирование электронного пропуска, смена замка);
- проверка надежности замков, установленных в защищаемых помещениях;
- имитация попытки проникновения в защищаемые помещения для проверки срабатывания сигнализации и (или) системы контроля и управления доступом.

3.10 Контрольные мероприятия в подсистеме криптографической защиты

При проведении контрольных мероприятий в подсистеме криптографической защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации.
- проверка сохранности эксплуатационной и технической документации и ключевых документов на средства криптографической защиты;
- проверка журналов учета средств криптографической защиты и используемых криптоключей на правильность их ведения и хранения;
- проверка знаний работниками, использующими средства криптографической защиты, правил применения этих средств и правил обращения с криптоключами;
- проверка функционирования средств криптографической защиты путем имитации процессов, шифрования и дешифрования информации.

**Рекомендации по составлению уведомления в уполномоченный
орган по защите прав субъектов персональных данных об
осуществлении обработки персональных**

**РЕКОМЕНДАЦИИ
ПО ЗАПОЛНЕНИЮ ОБРАЗЦА ФОРМЫ УВЕДОМЛЕНИЯ
ОБ ОБРАБОТКЕ (О НАМЕРЕНИИ ОСУЩЕСТВЛЯТЬ ОБРАБОТКУ)
ПЕРСОНАЛЬНЫХ ДАННЫХ МАОУ Мальковской СОШ**

1. Настоящие Рекомендации разработаны на основании приказа Роскомнадзора от 19 августа 2011 г. № 706 в целях заполнения уведомления об обработке (о намерении осуществлять обработку) персональных данных (далее - Уведомление) для регистрации Оператора персональных данных в реестре операторов Роскомнадзора.

2. Уведомление оформляется на официальном бланке МАОУ Мальковской СОШ (по форме, прилагаемой к настоящим Рекомендациям), осуществляющего обработку персональных данных, и направляется в территориальный орган Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Тюменской области (далее - территориальный орган Роскомнадзора).

3. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом.

4. В поле «наименование (фамилия, имя, отчество), адрес Оператора» указывается:

- полное наименование с указанием организационно-правовой формы и сокращенное наименование юридического лица, осуществляющего обработку персональных данных;
- адрес МАОУ Мальковской СОШ¹;

При указании наименования (фамилии, имени, отчества), адреса МАОУ Мальковской СОШ, а также направления деятельности рекомендуется использовать также ссылки на код(ы) классификаторов (ОКВЭД, ОКПО, ОКОГУ, ОКОП, ОКФС).

5. В поле «цель обработки персональных данных» указываются цели обработки персональных данных (а также их соответствие полномочиям МАОУ Мальковской СОШ). Под «целью обработки персональных данных» понимаются как цели, указанные в учредительных документах МАОУ Мальковской СОШ, так и цели фактически осуществляемой МАОУ Мальковской СОШ деятельности по обработке персональных данных в соответствии с Перечнем персональных данных, обрабатываемых в МАОУ Мальковской СОШ.

6. В поле «категории персональных данных» указываются все категории персональных данных, подлежащих обработке:

6.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

6.2. Специальные категории персональных данных (состояние здоровья, интимной жизни).

7. В поле «категории субъектов, персональные данные которых обрабатываются» указываются категории субъектов (физических лиц) в соответствии с Перечнем персональных данных, обрабатываемых в МАОУ Мальковской СОШ и виды отношений с субъектами (физическими лицами), персональные данные которых обрабатываются (например: работники(субъекты), состоящие в трудовых отношениях с юридическим лицом МАОУ Мальковской СОШ, и их родственники, физические лица (пациент и его родственники и др.) и др.).

8. В поле «правовое основание обработки персональных данных» указываются правовые основания согласно Перечню персональных данных, обрабатываемых в МАОУ Мальковской СОШ.

9. В поле «перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных», указываются действия, совершаемые МАОУ Мальковской СОШ с персональными данными, а также описание используемых МАОУ Мальковской СОШ способов обработки персональных данных, например: «смешанная обработка персональных данных (информация передается с использованием сети общего пользования Интернет по защищенным каналам связи)».

1 - Указывается место нахождения юридического лица в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, почтовый адрес юридического лица, контактная информация.

10. В поле «описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», указываются:

10.1. описание мер, предусмотренных ст.ст. 18.1 и 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

10.2. фамилия, имя, отчество работника, ответственного в МАОУ Мальковской СОШ за организацию обработки персональных данных, номер его контактного телефона, почтовый адрес и адрес электронной почты;

10.3. категорирование информационной системы персональных данных «наименование ИСПДн» МАОУ Мальковской СОШ (пункт 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» утвержденных Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119).

10.4. организационные и технические меры, применяемые для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных.

В случае использования МАОУ Мальковской СОШ, осуществляющим обработку персональных данных, шифровальных (криптографических) средств указываются следующие сведения:

10.5. наименование, регистрационные номера и производителей используемых криптографических средств;

10.6. уровень криптографической защиты персональных данных;

10.7. уровень специальной защиты от утечки по каналам побочных излучений и наводок;

10.8. уровень защиты от несанкционированного доступа.

Предоставление данной информации осуществляется в соответствии с Методическими рекомендациями по обеспечению с помощью крипто средств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденным руководством 8-го Центра Федеральной службы безопасности Российской Федерации 21 февраля 2008 г. № 149/5-144.

11. В поле «сведения о наличии или об отсутствии трансграничной передачи персональных данных» указываются сведения об отсутствии трансграничной передачи персональных данных в процессе их обработки.

12. В поле «сведения об обеспечении безопасности персональных данных» указываются сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

13. В поле «дата начала обработки персональных данных» указывается конкретная дата (число, месяц, год) начала любого действия (операции) или совокупность действий (операций), 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 (фактическая дата начала обработки персональных данных).

14. В поле «срок или условие прекращения обработки персональных данных» указывается конкретная дата (число, месяц, год) или основание (условие), наступление которого повлечет прекращение обработки персональных данных.

ПРИЛОЖЕНИЕ 1. ФОРМА УВЕДОМЛЕНИЯ

Руководителю Управления
Роскомнадзора по Тюменской
области

Уведомление об обработке (о намерении осуществлять обработку) персональных данных

	(полное и сокращенное наименования, фамилия, имя, отчество оператора)
руководствуясь:	(адрес местонахождения и почтовый адрес оператора)
	(правовое основание обработки персональных данных)
с целью:	(цель обработки персональных данных)
осуществляет обработку:	(категории персональных данных)
принадлежащих:	(категории субъектов, персональные данные которых обрабатываются)
Обработка вышеуказанных персональных данных будет осуществляться путем:	(перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных)
Для обеспечения безопасности персональных данных принимаются следующие меры:	(описание мер, предусмотренных ст.ст.18.1 и 19 Федерального закона N 152-ФЗ от 27.07.2006 "О персональных данных" в т.ч. сведения о наличии шифровальных (криптографических) средств и наименования этих средств; фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты)
Сведения о наличии или об отсутствии трансграничной передачи персональных данных:	(при наличии трансграничной передачи персональных данных в процессе их обработки, указывается перечень иностранных государств, на территорию которых осуществляется трансграничная передача персональных данных)
Сведения об обеспечении безопасности персональных данных:	(сведения об обеспечении безопасности персональных данных в соответствии с требованиями)

к защите персональных данных, установленными Правительством Российской Федерации)

Дата начала обработки персональных
данных

(число, месяц, год)

Срок или условие прекращения обработки персональных данных:

(число, месяц, год или основание (условие), наступление которого повлечет прекращение

обработки персональных данных)

(должность)

(подпись)

расшифровка подписи

" ____ " _____ 20 ____ г.

ПРИЛОЖЕНИЕ 2. ТИПОВАЯ ФОРМА УВЕДОМЛЕНИЯ ДЛЯ МУНИЦИПАЛЬНОГО ОРГАНА

Исх. № ____ от « ____ » _____ 20__ г.

Руководителю Управления Федеральной службы
по надзору в сфере связи, информационных технологий и
массовых коммуникаций
По Тюменской области

Уведомление
об обработке (о намерении осуществлять обработку) персональных
данных

Полное
наименование: _____
Сокращенное _____
наименование:

Адрес местонахождения (почтовый адрес) Оператора: 43XXXX, Ульяновская область, XXXXX, ул. XXXXXX, д.
XX
(Тел./Факс/E-mail): (XXXXX) XXXXX / (XXXXX) XXXXX /XXXXXXXXXXXXX.
(полное и сокращенное наименование, фамилия, имя, отчество)
(адрес местонахождения, почтовый адрес Оператора)

ИНН: XXXXXXXXXX КПП: XXXXXXXXXX ОГРН: XXXXXXXXXXXXXXXX
руководствуясь Конституцией Российской Федерации; Федеральным законом от 27.07.2006 №152-ФЗ
«О персональных данных»; ст.ст. 85-90 Трудового кодекса Российской Федерации (Федерального закона от
30.12.2001 №197-ФЗ), Федеральным законом от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений
граждан Российской Федерации»; Федеральным законом от 06.10.2003 № 131-ФЗ "Об общих принципах
организации местного самоуправления в Российской Федерации"; Уставом XXXXXXXX (утвержден
XX.XX.XXXXг.)

с целью обработки, регистрации сведений, необходимых для реализации полномочий органа местного
самоуправления, персональных данных работников, сведений об их профессиональной служебной деятельности.
(правовое основание обработки персональных данных)
(цель обработки персональных данных)

осуществляет обработку следующих категорий персональных данных:
фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия,
доходы, ИНН, паспортные данные, сведения о воинском учете, страховое свидетельство обязательного пенсионного
страхования;
(категории персональных данных)

принадлежащ _____ работникам (субъектам), состоящих в трудовых отношениях с юридическим лицом
их: _____ (оператором),
физическим лицам, состоящим в договорных и иных гражданско-правовых отношениях с юридическим лицом
(оператором).
(категории субъектов, персональные данные которых обрабатываются)

Обработка вышеуказанных персональных данных будет осуществляться путем: сбора, записи, систематизации,
накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения,
предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных.

Смешанная обработка вышеуказанных персональных данных будет осуществляться на
бумажных носителях и с использованием ПЭВМ с передачей полученной информации по внутренней
сети оператора и с передачей информации по сети общего пользования Интернет.

Для обеспечения безопасности персональных данных принимаются следующие меры:
Приказом ответственным за организацию обработки персональных данных назначен(о):
(перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных)

Иванов Иван Иванович
контактная информация: (8422)000000, 43XXXX, г. Ульяновск, ул. Почтовая, д. X, XXXXX@mail.ru
(Ф.И.О. физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных)
(номер телефона, ответственного за организацию обработки персональных данных, почтовый адрес и адрес электронной почты)

Применяются организационные и технические меры по обеспечению защиты персональных
данных с учетом актуальных угроз безопасности персональных данных и информационных
технологий, используемых в информационной системе: приняты локальные акты по вопросам
обработки персональных данных; ведется учет машинных носителей персональных данных;
осуществляется контроль за применяемыми мерами по обеспечению защиты персональных данных.
Персональные данные доступны лишь для строго определенных сотрудников оператора. Хранение
сведений (базы данных) организовано на электронных носителях с паролем, на бумажных носителях

- в сейфе. Шифрование не используется. Класс информационной системы персональных данных оператора: К_ (выбрать из перечисленного-К1 или К2, К3, К4 или система не классифицирована).

Средства обеспечения безопасности: пароли, разграничение доступа, использование средств антивирусной защиты.

(описание мер, предусмотренных ст.ст. 18.1 и 19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», в т.ч. сведения о наличии шифровальных (криптографических) средств и наименование этих средств; фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты)

Сведения о наличии или об отсутствии трансграничной передачи персональных данных: не осуществляется.

(при наличии трансграничной передачи персональных данных в процессе их обработки, указывается перечень иностранных государств, на территорию которых осуществляется трансграничная передача персональных данных)

Сведения об обеспечении безопасности персональных данных:

Актом руководителя утверждены документы: правила обработки персональных данных; правила рассмотрения запросов субъектов персональных данных или их представителей; правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных; правила работы с обезличенными данными; перечень информационных систем персональных данных; перечни персональных данных, обрабатываемых в учреждении в связи с реализацией трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением возложенных полномочий; перечень должностей служащих, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных; перечень должностей служащих, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным; должностная инструкция ответственного за организацию обработки персональных данных в учреждении; типовое обязательство служащего, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним муниципального контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей; типовая форма согласия на обработку персональных данных работников, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные; порядок доступа служащих в помещения, в которых ведется обработка персональных данных.

Служащие, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных. Установлен уровень защищенности персональных данных при их обработке в информационной системе; назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе; утвержден перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей; организован режим обеспечения безопасности помещения, в котором размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этом помещении лиц, не имеющих права доступа в это помещение; обеспечена сохранность носителей персональных данных.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации, проинформированы об особенностях и правилах осуществления такой обработки, локальными актами установлены места хранения персональных данных и перечень лиц осуществляющих обработку персональных данных.

(сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации)

Дата начала обработки персональных данных:

(указывается дата регистрации юридического лица)

XX.XX.XXXXг.

(число, месяц, год)

Срок или условия прекращения обработки персональных данных:

прекращение деятельности как юридического лица.

Директор

(должность)

(подпись)

(фамилия, имя, отчество)

М.П.

“ 20 г.
”
(число) (м) (г)
 (есяц) (од)

Исп.:
Тел.:

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКА

Я, _____,
(Ф.И.О.)

Проживающий по адресу: _____

Паспорт № _____, выданный _____ (кем _____ и _____
когда) _____

настоящим даю свое согласие на обработку в _____

(наименование и юридический адрес МАОУ Мальковской СОШ)

моих персональных данных, к которым относятся:

- паспортные данные;
- данные страхового Свидетельства государственного пенсионного страхования;
- данные документа воинского учета¹;
- документы об образовании, профессиональной переподготовке, повышении квалификации, стажировки, присвоении ученой степени, ученого звания (если таковые имеются);
- анкетные данные, предоставленные мною при поступлении на работу или в процессе работы (в том числе - автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);
- данные иных документов, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены мною при заключении трудового договора или в период его действия²;
- данные трудового договора и соглашений к нему;
- данные кадровых приказов о моем приеме, переводах, увольнении;
- данные личной карточки по формам Т-2 и Т-1;
- данные документов о прохождении мной аттестации, собеседования, повышения квалификации, результатов оценки и обучения;
- фотография;
- иные сведения обо мне, которые необходимо МАОУ Мальковской СОШ для корректного документального оформления правоотношений между мною и МАОУ Мальковской СОШ.

Я даю согласие на использование моих персональных данных в целях:

- корректного документального оформления трудовых правоотношений между мною и МАОУ Мальковской СОШ;
- обеспечения выполнения мною должностных обязанностей (трудовой функции);
- предоставления информации в государственные органы Российской Федерации в порядке, предусмотренном действующим законодательством;
- предоставления информации в медицинские учреждения, страховые компании;

¹ Только для военнообязанных и лиц, подлежащих призыву на военную службу.

² Например, медицинские заключения, при прохождении обязательных предварительных и периодических медицинских осмотров и т.д.

– обеспечения предоставления мне социального пакета.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу третьим лицам, медицинским учреждениям и т.д.), обезличивание, блокирование, трансграничную передачу персональных данных, а также осуществление любых иных действий с моими персональными данными, предусмотренных действующим законодательством Российской Федерации.

МАОУ Мальковской СОШ гарантирует, что обработка моих личных данных осуществляется в соответствии с действующим законодательством РФ и «Положением о защите персональных данных работников МАОУ Мальковской СОШ», с которым я ознакомлен (а) при трудоустройстве в МАОУ Мальковской СОШ.

Данное Согласие действует с момента заключения мною Трудового договора с МАОУ Мальковской СОШ и до истечения сроков, установленных действующим законодательством Российской Федерации.

Я подтверждаю, что, давая такое Согласие, я действую своей волей и в своих интересах.

Так же мне разъяснены юридические последствия отказа предоставить свои персональные данные МАОУ Мальковской СОШ.

В соответствии со статьями 26, 42 Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации», Положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденного Указом Президента Российской Федерации от 30 мая 2005 г. № 609, определен перечень персональных данных, которые субъект персональных данных обязан предоставить в связи с поступлением на государственную гражданскую службу.

Без представления субъектом персональных данных обязательных для заключения служебного контракта сведений, служебный контракт не может быть заключен.

Дата: _____ Подпись _____ / _____ - /