**УТВЕРЖДАЮ**
**Заведующая МДОУ Тисульского**
**детского сада № 4**
**_____ О.М. Ефимова**
Приказ № 114 от 15.11.2018

**ПРАВИЛА**
осуществления внутреннего контроля соответствия обработки персональных данных
требованиям к защите персональных данных
в МДОУ Тисульском детском саде № 4

Пгт. Тисуль
2018 г.

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в муниципальном дошкольном образовательном учреждении Тисульском детском саде № 4 (далее МДОУ) разработаны в соответствии с:

– Постановлением Правительства Российской Федерации от 21 марта 2012 г. №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»;

– Постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Нормативно-методическим документом «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденного Приказом Государственной технической комиссии при Президенте Российской Федерации от 30.08.2002 г. №282;

– Приказом ФСТЭК России от 20.03.2012 г. № 28 «Требования к средствам антивирусной защиты»;

– Приказом ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказом ФСТЭК России от 06.12.2011 г. № 638 «Требования к системам обнаружения вторжений»

в целях выполнения требований к защите персональных данных, установленных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативными правовыми актами и локальными актами МДОУ (далее – оператор).

2. Оператор в целях выполнения требований к защите персональных данных, установленных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или 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.

3. Целью проведения контроля является оценка соответствия обработки персональных данных требованиям по обеспечению безопасности персональных данных и обеспечение уровня защищенности информационных систем персональных данных.

4. При обработке персональных данных контролируемыми показателями являются:

– угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;

– выполнение 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;

– наличие, ведение, состояние учёта и выполнение правил эксплуатации, прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– наличие, ведение, состояние ведения учета машинных носителей персональных данных;
– правомерность доступа к персональным данным;
– выполнение решений по предотвращению несанкционированного доступа к персональным данным с применением организационных и технических мер;
– обеспеченность возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
– выполнение правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных.

5. Объектами контроля являются:
– информационные системы персональных данных, в которых осуществляется обработка персональных данных ограниченного доступа;
– информационные системы, в которых осуществляется обработка обезличенных персональных данных.

6. Контроль проводится:
– ответственными за эксплуатацию информационных систем персональных данных;
– администраторами безопасности информационных систем персональных данных;
– уполномоченным лицом, ответственным за организацию и проведение контроля и комиссией, назначенными приказом по МДОУ;
– организациями, имеющими лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

7. Формами контроля являются:
– текущий контроль, осуществляемый администратором безопасности информационных систем персональных данных в соответствии с инструкциями;
– периодический контроль, организуемый и проводимый уполномоченным лицом, назначенным приказом по МДОУ, в отношении информационных систем персональных данных, в которых осуществляется обработка персональных данных ограниченного доступа, а также информационных систем, в которых осуществляется обработка обезличенных персональных данных, и иных информационных систем информационной инфраструктуры МДОУ;
– внеплановый контроль, организуемый и проводимый уполномоченным лицом, назначенным приказом по МДОУ, с привлечением при необходимости специалистов из числа работников учреждения.
– комплексный контроль за выполнением установленных требований к защите персональных данных, организуемый и проводимый оператором самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

8. Регистрация результатов контроля осуществляется в Журнале регистрации контрольных мероприятий по выполнению требований по защите персональных данных МДОУ (Приложение № 1) лицами, уполномоченными на организацию и проведение соответствующего вида контроля.

9. Регламент проведения текущего контроля

| **Должностное лицо (функция)** | **Контролируемые показатели (осуществляемые действия)** | **Периодичность контроля** | **Форма регистрации** | **Действия при выявлении нарушений** |
|---|---|---|---|---|
| Ответственный за эксплуатацию информационной системы персональных данных | доступ лиц в помещения, в которых размещены средства обработки персональных данных | непрерывно | Запись в журнале учёта сотрудников и посетителей | Служенная записка руководителю (ответственному за обеспечение безопасности) |
| | доступ пользователей и администратора защиты информации к средствам вычислительной техники информационной системы персональных данных | непрерывно | Запись в журнале учёта рабочего времени пользователей | Служенная записка руководителю (ответственному за обеспечение безопасности) |
| | наличие журналов учёта технической, эксплуатационной и аттестационной документации | еженедельно | Запись в журнале регистрации контрольных мероприятий | Служенная записка руководителю (ответственному за обеспечение безопасности) |
| | наличие эксплуатационной документации (инструкций, положений) | еженедельно | Запись в журнале регистрации контрольных мероприятий | Служенная записка руководителю (ответственному за обеспечение безопасности) |
| | состав средств защиты информации | ежемесячно | Запись в журнале регистрации контрольных мероприятий | Служенная записка руководителю (ответственному за обеспечение безопасности) |
| | состав программных средств обработки персональных данных | ежемесячно | Запись в журнале регистрации контрольных мероприятий | Служенная записка администратору защиты информации |
| | состав технических средств обработки персональных данных, соответствие расположения технических средств данным технического паспорта информационной системы персональных данных | ежемесячно | Запись в журнале регистрации контрольных мероприятий | Служенная записка руководителю (ответственному за обеспечение безопасности) |
| | выполнение пользователями требований инструкций по обеспечению безопасности персональных данных | непрерывно | Запись в журнале регистрации контрольных мероприятий о выявленных фактах нарушений | Служенная записка администратору защиты информации |

| Должностное лицо (функция) | Контролируемые показатели (осуществляемые действия) | Периодичность контроля | Форма регистрации | Действия при выявлении нарушений |
|---|---|---|---|---|
| | состояние технических средств защиты помещений, охранной, пожарной сигнализации | ежедневно | Запись в журнале регистрации контрольных мероприятий о выявленных фактах несоответствия | Служенная записка руководителю (ответственному за обеспечение безопасности) |
| | наличие зарегистрированных машинных носителей информации | ежедневно | Запись в журнале регистрации контрольных мероприятий о выявленных фактах нарушений | Служенная записка руководителю (ответственному за обеспечение безопасности) |
| | целостность мастичных печатей (опломбирования) системных блоков средств вычислительной техники | ежедневно | Запись в журнале регистрации контрольных мероприятий о выявленных фактах нарушений | Служенная записка руководителю (ответственному за обеспечение безопасности) |
| | соответствие грифа конфиденциальности машинного носителя информации степени конфиденциальности записанной на носителе информации | еженедельно | Запись в журнале регистрации контрольных мероприятий о выявленных фактах нарушений | Служенная записка руководителю (ответственному за обеспечение безопасности) |
| Администратор защиты информации | проверка (по журналу аудита системных событий системы защиты от несанкционированного доступа (НСД)) целостности и неизменности основных системных ресурсов операционной системы, конфигурации и настроек компьютеров, целостности и неизменности файлов системы защиты от НСД | ежемесячно | Запись в журнале регистрации контрольных мероприятий о выявленных фактах нарушений | Запрет работы на Объекте информатизации.<br>Проведение анализа и выявления причин несанкционированного доступа.<br>Устранение выявленных ошибки и уязвимости.<br>Обновление контрольных сумм контролируемых ресурсов.<br>Служенная записка руководителю (ответственному за обеспечение безопасности). |
| | оценка возможности подключения к | еженедельно | Запись в журнале | Запрет работы на Объекте |

| Должностное лицо (функция) | Контролируемые показатели (осуществляемые действия) | Периодичность контроля | Форма регистрации | Действия при выявлении нарушений |
|---|---|---|---|---|
| | защищаемым средствам ВТ нештатных устройств считывания информации (дискеты, DVD/CD-диски, USB-устройства) | | регистрации контрольных мероприятий о выявленных фактах нарушений | информатизации. Проведение анализа и выявления причин несанкционированного подключения. Устранение выявленных нарушений Служенная записка руководителю (ответственному за обеспечение безопасности). |
| | оценка возможности подключения к защищаемым средствам ВТ модемов, других ПЭВМ, Интернет, Wi-Fi, Bluetooth, и др | еженедельно | Запись в журнале регистрации контрольных мероприятий о выявленных фактах нарушений | Запрет работы на Объекте информатизации. Проведение анализа и выявления причин несанкционированного подключения. Устранение выявленных нарушений. Служенная записка руководителю (ответственному за обеспечение безопасности). |
| | права доступа пользователей к информационным ресурсам | ежедневно | Запись в журнале регистрации контрольных мероприятий о выявленных фактах нарушений | Запрет работы на Объекте информатизации. Проведение анализа и выявления причин нарушения прав доступа. Устранение выявленных нарушений прав доступа. Служенная записка руководителю (ответственному за обеспечение безопасности). |

10. Регламент проведения периодического контроля

10.1. Периодический контроль предусматривает оценку достаточности и эффективности мероприятий по организационному и техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных и включает оценку:

– угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– эффективности выполнения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

– наличия, ведения учёта средств защиты информации и выполнения правил по их эксплуатации;
– состояния ведения учета машинных носителей персональных данных;
– выполнения решений по предотвращению несанкционированного доступа к персональным данным с применением организационных и технических мер;
– возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
– выполнения правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
– выполнения требований по обезличиванию персональных данных и их обработке в информационных системах.

10.2. Периодический контроль соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» проводится не реже одного раза в год.

10.3. Для целей осуществления периодического контроля 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. 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.

10.4. Объектами периодического контроля являются все информационные системы информационной инфраструктуры МДОУ.

10.5. В ходе периодического контроля должны оцениваться:
– соответствие фактического состава обрабатываемых персональных данных в информационных системах персональных данных составам персональных данных, утверждённых для соответствующих информационных систем персональных данных;
– состав информационных ресурсов информационных систем, обрабатывающих обезличенные персональные данные;
– состав информационных ресурсов информационных систем, не включенных в утверждённый перечень информационных систем персональных данных Комитета на предмет выявления фактов обработки персональных данных;
– соответствие фактических технологий обработки персональных данных в информационных системах персональных данных утверждённым технологиям;
– наличие, достаточность и соответствие разработанной документации по защите персональных данных требованиям по защите персональных данных в реальных условиях эксплуатации информационных систем персональных данных;
– соответствие фактических угроз безопасности персональным данным при их обработке в информационных системах персональных данных угрозам, приведённым в Моделях угроз безопасности персональным данным при их обработке в информационных системах персональных данных;
– состав основных и вспомогательных технических средств и систем информационных систем персональных данных, средств защиты информации, общесистемного и прикладного программного обеспечения;
– соответствие разрешительной системы доступа установленной;
– порядок учёта и использования машинных носителей информации:

– полнота выполнения должностных обязанностей и уровень подготовки лиц ответственных за эксплуатацию и администраторов защиты информации информационных систем персональных данных;
– полнота, периодичность проведения текущего контроля ответственными за эксплуатацию и администраторами защиты информации информационных систем персональных данных;
– полнота выполнения должностных обязанностей ответственных за обезличивание персональных данных;
– полнота выполнения обязанностей лиц, осуществляющих обработку персональных данных;
– наличие, состояние и порядок учёта согласий граждан на обработку персональных данных;
– возможность доступа граждан к Порядку обработки персональных данных, устанавливающему процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющих для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;
– эффективность применяемых средств защиты информации;
– состояние антивирусной защиты в информационных системах персональных данных.

10.6. При выявлении в ходе проведения периодического контроля изменений, которые могут повлечь снижение заданного уровня защищённости персональных данных в информационных системах персональных данных, проводится контроль защищённости персональных данных от утечки по техническим каналам с использованием специализированных средств измерений и контроля с оформлением протоколов по оценки защищённости персональных данных и (или) эффективности мер и средств защиты персональных данных в информационных системах персональных данных.

10.7. По результатам периодического контроля лицом, уполномоченным на организацию и проведение периодического контроля, и членами комиссии составляется заключение по результатам контроля, содержащее результаты оценки по показателям, приведённым в п. 10.5, выводы о соответствии (несоответствии) состояния защищённости персональных данных установленному уровню защищённости, рекомендации по устранению выявленных недостатков и нарушений и сроков их устранения, подписываемое указанными выше лицами и представляемое на утверждение председателя Комитета.

11. Регламент внепланового контроля

11.1. Внеплановый контроль проводится в случаях:

11.1.1. выявления фактов незаконного разглашения (распространения) персональных данных;

11.1.2. подачи гражданами жалоб на нарушение их прав на неприкосновенность личности в части обработки персональных данных;

11.1.3. при изменении хотя бы одной из следующих характеристик:

- состав обрабатываемых персональных данных;
- технология обработки персональных данных;
- применяемые меры и средства защиты персональных данных;
- общесистемное и (или) прикладное программное обеспечение;
- состав основных технических средств и систем;
- состав средств защиты информации;
- права и полномочия субъектов доступа к информационным ресурсам ИСПДн.

11.2. Внеплановый контроль проводится в обязательном порядке на основании служебных записок руководителю (ответственному за обеспечение безопасности) или администратору безопасности АС.

11.3. Решение о проведении внепланового контроля принимает руководитель или его заместитель по режиму (безопасности).

11.4. Внеплановый контроль организуется и проводится уполномоченным лицом, назначенным приказом МДОУ, с привлечением при необходимости специалистов из числа работников МДОУ. По результатам внепланового контроля составляется заключение, содержащее перечень оцениваемых показателей, оценку причин выявленных нарушений и (или) несоответствий, состав принятых по устранению нарушений и (или) несоответствий мер, представляемое на утверждение заведущему МДОУ Тисульского детского сада № 4.

11.5. По фактам незаконного разглашения (распространения) персональных данных в обязательном порядке проводится служебное расследование.

12. Регламент проведения комплексного контроля

12.1. Комплексный контроль над выполнением требований к защите персональных данных, установленных Федеральным законом «О персональных данных», организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации, не реже одного раза в три года.

12.2. Целью комплексного контроля является оценка достаточности выбранных и реализованных в системе защиты персональных данных организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных проводится не реже, чем раз в три года при условии неизменности состава средств обработки информации, технологии обработки информации, средств защиты информации, класса защиты автоматизированной системы от несанкционированного доступа, класса защиты ИСПДн и уровня защищённости ИСПДн.

12.3. Комплексный контроль проводится также в случаях изменения состава средств обработки информации, технологии обработки информации, средств защиты информации, класса защиты автоматизированной системы от несанкционированного доступа, класса защиты ИСПДн и уровня защищённости ИСПДн.

12.4. Объектами комплексного контроля являются все информационные системы персональных данных

12.5. Комплексный контроль осуществляется по оценке показателей и в порядке, установленных соответственно п. 10.1 и 10.3 с обязательным проведением контрольных мероприятий по оценке защищённости персональных данных от утечки по техническим каналам, эффективности применяемых средств защиты информации с использованием специализированных средств измерений и контроля с оформлением протоколов по оценки защищённости персональных данных и (или) эффективности мер и средств защиты персональных данных в информационных системах персональных данных.

12.6. По решению заведующей МДОУ комплексный контроль может быть проведён в форме аттестации ИСПДн по требованиям безопасности информации.

12.7. Комплексный контроль форме аттестации ИСПДн по требованиям безопасности информации проводится организациями, имеющими лицензии ФСТЭК России на деятельность в области технической защиты конфиденциальной информации, дающей право на аттестацию объектов информатизации, в соответствии с разработанной для соответствующей информационной системы персональных данных

Программой и методиками аттестации объекта вычислительной техники требованиям по безопасности информации.

12.8. Аттестация информационных систем персональных данных проводится по указанной в п. 12.7 Программе до полного завершения всех предусмотренных Программой мероприятий независимо от получаемых промежуточных результатов.

12.9. По результатам аттестационных испытаний информационных систем персональных данных и на основании вывода о соответствии (не соответствии) выбранных и реализованных в системе защиты персональных данных организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных, оформляемых протоколами контроля защищённости (оценки эффективности), составляется Заключение по результатам аттестационных испытаний, и на основании вывода в котором выдаётся (не выдаётся) аттестат соответствия требованиям по безопасности информации информационной системы персональных данных.

12.10. Аттестат соответствия требованиям по безопасности информации информационной системы персональных данных выдаётся на срок, не превышающий три года при условии неизменности состава средств обработки информации, технологии обработки информации, средств защиты информации, класса защиты автоматизированной системы от несанкционированного доступа, класса защиты ИСПДн и уровня защищённости ИСПДн.

12.11. По истечении срока действия Аттестата соответствия переаттестация информационной системы персональных данных не проводится. Возобновление действия Аттестата соответствия проводится в порядке, установленном для аттестации.