АДМИНИСТРАЦИЯ ТОНШАЕВСКОГО
МУНИЦИПАЛЬНОГО ОКРУГА НИЖЕГОРОДСКОЙ
ОБЛАСТИ

Муниципальное дошкольное образовательное учреждение детский сад №15 «Ромашка»

(МДОУ детский сад №15 «Ромашка»)

ПРИКАЗ

«27» мая 2025 г. № 79-од

р.п. Пижма

Об утверждении Положения об обеспечении безопасности персональных данных

В соответствии со статьей 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» п р и к а з ы в а ю:

1. Утвердить прилагаемое Положение об обеспечении безопасности персональных данных.
2. Контроль за исполнением настоящего приказа остается за заведующим учреждением.

Заведующий **Н.А. Овчинникова**

Приложение

УТВЕРЖДЕНА
приказом МДОУ детского сада №15
«Ромашка»
от «27» мая 2025 г. № 79-од

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных

1. Общие положения

1.1. Настоящее Положение определяет порядок выработки правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в Муниципальном дошкольном образовательном учреждении детском саду №15 «Ромашка» (далее – учреждение, оператор).

1.2. Термины и определения, используемые в Положении, подлежат применению и толкованию в значении, установленном:

Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

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

В учреждении имеются следующие информационные системы персональных данных:

персональные компьютеры,

система видеонаблюдения.

Персональные компьютеры, в свою очередь, содержат информационные системы – программное обеспечение. Всё установленное программное обеспечение является сертифицированным и лицензионным.

В отношении каждой системы проводится классификация для установления уровня защищенности. По итогам классификации для ИСПД устанавливается уровень защищенности персональных данных.

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

В учреждении, с учетом требований приказа ФСТЭК России 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» применяются следующие меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных:

идентификация и аутентификация субъектов доступа и объектов доступа;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

антивирусная защита;

контроль (анализ) защищенности персональных данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них.

4. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации

На ИСПД – персональных компьютерах имеется антивирусная защита.

5. Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных

Перед установкой информационной системы персональных данных проводилось изучение данных антивирусной защиты.

6. Учет машинных носителей персональных данных

Поскольку оператор персональных данных является муниципальным учреждением, машинные носители персональных данных отнесены к особо ценному движимому имуществу и подлежат особому учету.

7. Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них

Учреждением введен режим готовности к обнаружению несанкционированного доступа к персональным данным. С работниками, осуществляющими обработку персональных данных, проведена разъяснительная работа о необходимости оперативного реагирования на утечки ПД.

С работников учреждения, имеющих доступ к персональным данным, взяты обязательства о неразглашении персональных данных.

8. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним

Учреждением предпринимаются меры резервного копирования ИСПД.

9. Установление 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

Приказом учреждения установлен список работников учреждения, имеющих доступ к персональным данным. Каждому работнику для аутентификации в ИСПД выдан логин и пароль.

10. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Один раз в три года учреждением проводится внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных. По итогам внутреннего контроля составляется соответствующий акт, подтверждающий осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону «О персональных данных».

_____