

АДМИНИСТРАЦИЯ ТОНШАЕВСКОГО
МУНИЦИПАЛЬНОГО ОКРУГА НИЖЕГОРОДСКОЙ
ОБЛАСТИ

**Муниципальное дошкольное образовательное
учреждение детский сад №15 «Ромашка»**

(МДОУ детский сад №15 «Ромашка»)

ПРИКАЗ

«27» мая 2025 г.

№ 78-од

р.п. Пижма

**Об утверждении Правил
осуществления внутреннего контроля
соответствия обработки
персональных данных
в информационных системах
персональных данных требованиям
к защите персональных данных**

В соответствии с пунктом 2 части 1 статьи 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», пунктом 17 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, п р и к а з ы в а ю:

1. Утвердить прилагаемые Правила осуществления внутреннего контроля соответствия обработки персональных данных в информационных системах персональных данных требованиям к защите персональных данных.

2. Контроль за исполнением настоящего приказа остается за заведующим учреждением.

Заведующий

Н.А. Овчинникова

Приложение

УТВЕРЖДЕНЫ
приказом МДОУ детского сада №15
«Ромашка»
от «27» мая 2025 г. № 78-од

ПРАВИЛА осуществления внутреннего контроля соответствия обработки персональных данных в информационных системах персональных данных требованиям к защите персональных данных

1. Настоящие правила регламентируют порядок осуществления внутреннего контроля соответствия обработки персональных данных в информационных системах персональных данных требованиям к защите персональных данных (далее – контроль, внутренний контроль).
2. Целью внутреннего контроля является предотвращение и выявление нарушений законодательства Российской Федерации в сфере персональных данных, устранение последствий таких нарушений.
3. Внутренний контроль проводится на основании приказа учреждения.
4. При проведении контроля учреждение руководствуется нормативными правовыми актами Российской Федерации, регламентирующими работу с персональными данными, а также Положением об организации работы с персональными данными в учреждении.
5. Предметом контроля являются:
 - проверка соответствия информационных систем персональных данных параметрам, указанным в актах классификации информационных систем персональных данных;
 - соблюдение работниками учреждения мер по защите персональных данных;
 - соблюдение организационных мер и средств защиты информации, обеспечивающих безопасную обработку персональных данных;
 - проверка соответствия сведений о лицах, допущенных к обработке персональных данных, и уровне их доступа;
 - проверка соответствия сведений о составе и структуре обрабатываемых персональных данных.
6. Плановый контроль осуществляется не реже одного раза в три года.
7. Внеплановый контроль осуществляется при наличии существенного нарушения функционирования работы в сфере персональных данных.
8. На время проведения контроля создается комиссия из числа работников учреждения.
9. Проверка информационной системы персональных данных включает:
 - наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена;
 - наличие резервных копий общесистемного программного обеспечения;
 - наличие резервных копий носителей персональных данных;
 - наличие информационных ресурсов (баз данных, файлов и других), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
 - проверку системы контроля физического доступа к информационной системе;

проверку существующих технологических мер защиты персональных данных;
проверку разграниченных прав доступа лиц к обрабатываемым персональным данным;
проверку состава и структуру объектов защиты;
проверку конфигурации и структуры информационной системы;
проверку режима обработки персональных данных;
проверку перечня лиц, участвующих в обработке персональных данных;
моделирование угроз безопасности персональных данных, оценку вероятность их реализации, реализуемость, опасность и актуальность.

10. По итогам проверки при необходимости:

вносятся изменения в План мероприятий по обеспечению защиты персональных данных;

уточняется перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним;

формируются новые модели угроз безопасности персональных данных;

составляется список необходимых мер защиты персональных данных;

вносятся изменения в локальные нормативные акты учреждения по вопросам обработки персональных данных.
