

ПРИНЯТО

Советом МБДОУ МО г.
Краснодар «Детский сад № 167»
Протокол № 5
от «30» августа 2023 г.

УТВЕРЖДАЮ

Заведующий МБДОУ МО г.
Краснодар «Детский сад № 167»
О.Б.Скляр
«30» августа 2023 г.



**Правила
осуществления внутреннего контроля
соответствия обработки персональных данных требованиям к защите
персональных данных в МБДОУ МО г. Краснодар «Детский сад № 167»**

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия

обработки персональных данных требованиям к защите персональных данных (далее - Правила контроля) в МБДОУ МО г. Краснодар «Детский сад № 167» определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных населения; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите персональных данных.

1.2. Настоящие Правила контроля разработаны на основании:

- Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»,
- Федерального закона Российской Федерации от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

в соответствии с частью 1 «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», утвержденных постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211.

1.3. МБДОУ МО г. Краснодар «Детский сад № 167» использует информационные системы персональных данных (далее - ИСПДн) для выполнения основных целей и задач обработки персональных данных, указанных в пункте 2 Положения по обработке и защите персональных данных.

1.4. Пользователями ИСПДн (далее - Пользователь) являются сотрудники МБДОУ МО г. Краснодар «Детский сад № 167», участвующие в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющие доступ к аппаратным средствам, программному обеспечению (далее - ПО), данным и средствам защиты информации (далее - СЗИ) ИСПДн.

1.5. Контрольные мероприятия по обеспечению уровня защищенности ПДн и

соблюдению условий использования СЗИ, а также соблюдению требований

законодательства Российской Федерации по обработке ПДн в ИСПДн МБДОУ МО г. Краснодар «Детский сад № 167» проводятся в следующих целях:

- проверка выполнения требований организационно-распорядительной документации по защите информации в МБДОУ МО г. Краснодар «Детский сад № 167» и действующего законодательства Российской Федерации в области обработки и защиты ПДн;

- оценка уровня осведомленности и знаний сотрудников МБДОУ МО г. Краснодар «Детский сад № 167» в области обработки и защиты персональных данных;

- оценка обоснованности и эффективности применяемых мер и средств защиты персональных данных.

2. Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите персональных данных

2.1. Проверки соответствия обработки ПДн установленным требованиям в МБДОУ МО г. Краснодар «Детский сад № 167» разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия периодически проводятся администратором ИС в соответствии с утвержденным планом (Приложение 1 к правилам осуществления внутреннего контроля соответствия обработки персональным данным требованиям к защите персональных данных, утверждено руководителем МБДОУ МО г. Краснодар «Детский сад № 167»)

проведения контрольных мероприятий (далее - План) и предназначены для осуществления контроля выполнения требований в области защиты информации в МБДОУ МО г. Краснодар «Детский сад № 167».

2.3. Плановые контрольные мероприятия периодически проводятся постоянной комиссией в соответствии с утвержденным Планом и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн МБДОУ МО г. Краснодар «Детский сад № 167» .

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

- по результатам расследования инцидента информационной безопасности;
- по результатам внешних контрольных мероприятий, проводимых регулирующими органами;
- по решению руководителя МБДОУ МО г. Краснодар «Детский сад № 167».

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий лицо,

ответственное за обеспечение безопасности персональных данных, разрабатывает план внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий 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.

3.3. 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.

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты

проверок фиксируется в журнале учета событий информационной безопасности (Приложение 2 к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных).

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий ответственное лицо или члены комиссии разрабатывают отчет, в котором указывается:

- описание проведенных мероприятий по каждому из этапов;

- перечень и описание выявленных нарушений;

- рекомендации по устранению выявленных нарушений;

- заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. Отчет передается на рассмотрение руководителю МБДОУ МО г. Краснодар «Детский сад № 167» .

4.4. Общая информация о проведенном контрольном мероприятии фиксируется в журнале учета событий информационной безопасности.

4.5. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите ПДн в МБДОУ МО г. Краснодар «Детский сад № 167» (Приложение 3 к Правилам осуществления внутреннего контроля соответствия обработки персональным данным требованиям к защите персональных данных).

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при

обязательном участии лица, ответственного за обеспечение безопасности персональных данных, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы ИС и ответственные за обеспечение безопасности ПДн информационных систем персональных данных..

5.2. Лицо, ответственное за обеспечение безопасности персональных данных , 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.

При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий в зависимости от целей мероприятий могут выполняться следующие проверки:

- соответствия полномочий Пользователя правилам доступа;
- соблюдения Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн;
- соблюдения администраторами ИСПДн инструкций и регламентов по обеспечению безопасности информации в МБДОУ МО г. Краснодар «Детский сад № 167» ;
- соблюдения порядка доступа сотрудников в помещения МБДОУ МО г. Краснодар «Детский сад № 167» , где ведется обработка персональных данных;
- знания Пользователями положений инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций;
- знание администраторами ИСПДн инструкций и регламентов по обеспечению безопасности информации в МБДОУ МО г. Краснодар «Детский сад № 167»;
- порядок и условия применения средств защиты информации;
- состояние учета машинных носителей ПДн;
- наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер;

- проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- технические мероприятия, связанные со штатным и нештатным функционированием средств защиты;

-технические мероприятия, связанные со штатным и нештатным функционированием подсистем системы защиты.

Приложение 1
к Правилам осуществления внутреннего контроля соответствия
обработки персональным данным требованиям к защите
персональных данных

**План внутреннего контроля соответствия обработки персональных данных
требованиям защиты персональных данных**

Мероприятие	Периодичность регулярных мероприятий	Периодичность плановых мероприятий	Исполнитель
Контроль соблюдения правил доступа к персональным данным	Еженедельно	Ежемесячно	Пользователи ИС, члены комиссии
Контроль соблюдения режима защиты	Еженедельно	Ежемесячно	Пользователи ИС, члены комиссии
Контроль выполнения антивирусной политики	Еженедельно	Ежемесячно	Пользователи ИС, члены комиссии
Контроль выполнения парольной политики	Еженедельно	Ежемесячно	Пользователи ИС, члены комиссии
Контроль соблюдения режима защиты при подключении к сетям общего пользования	Еженедельно	Ежемесячно	Пользователи ИС, члены комиссии
Выявление изменений в режиме обработки и защиты персональных данных	Еженедельно	Ежемесячно	Ответственный за обработку, защиту и хранение персональных данных
Контроль обновления ПО и единообразия применяемого ПО на всех элементах ИС	Еженедельно	Ежемесячно	Пользователи ИС, члены комиссии
Контроль обеспечения резервного копирования	Еженедельно	Ежемесячно	Пользователи ИС, члены комиссии
Организация анализа и пересмотра имеющихся угроз безопасности персональных данных, выявление новых угроз	Еженедельно	Ежемесячно	Пользователи ИС, члены комиссии
Актуализация нормативно-организационных документов	Еженедельно	По мере изменений действующего законодательств	Ответственный за обработку, защиту и хранение персональных

		ва	данных
Контроль использования беспроводных соединений	Еженедельно	Ежемесячно	Пользователи ИС, члены комиссии

Приложение 2
к Правилам осуществления внутреннего контроля соответствия
обработки персональным данным требованиям к защите
персональных данных

ЖУРНАЛ
учета событий информационной безопасности
МБДОУ МО г. Краснодар «Детский сад № 167»

№	Дата события	Основание возникновения события	Описание события (мероприятия)	Характеристика события	Ф.И.О. субъекта	Должность	Примечание

Приложение 3
к Правилам осуществления внутреннего контроля соответствия
обработки персональным данным требованиям к защите
персональных данных

ПРОТОКОЛ № _____
проведения внутреннего контроля соответствия обработки персональных данных
требованиям защиты персональных данных

Дата проведения проверки « _____ » _____ 20 _____ г.

Проверка проведена комиссией в составе:

Тема проверки: _____

Проверка осуществлялась в соответствии с требованиями _____

В ходе проверки
проверено: _____

выявлено: _____

Меры по устранению нарушений: _____

Срок устранения нарушений: _____

Председатель комиссии _____ / _____ /

Члены комиссии _____ / _____ /

_____ / _____ /