

Приложение № 3

к приказу
МДОУ «Ряжский детский сад № 1»
от 09.01.2025 № 1/72



ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МДОУ «Ряжский детский сад № 1»

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в МДОУ «Ряжский детский сад № 1» определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПДн.

1.2. Настоящие Правила разработаны на основании Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона РФ от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и 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 РФ от 21 марта 2012 г. № 211.

1.3. Для обработки персональных данных в МДОУ «Ряжский детский сад № 1» используются информационные системы, перечень которых утверждается руководителем управы (далее – информационные системы).

1.4. Пользователем информационной системы (далее – Пользователь) является работник МДОУ «Ряжский детский сад № 1», участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам,

программному обеспечению, данным и средствам защиты информации информационной системы.

1.5. Контрольные мероприятия 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 проводятся в следующих целях:

1.5.1 проверка выполнения требований организационно-распорядительной документации по защите информации в МДОУ «Ряжский детский сад № 1» и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.5.2 оценка уровня осведомленности и знаний работников МДОУ «Ряжский детский сад № 1» в области обработки и защиты персональных данных;

1.5.3 оценка обоснованности и эффективности применяемых мер и средств защиты информации.

2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1. Проверки соответствия обработки ПДн установленным требованиям в МДОУ «Ряжский детский сад № 1» разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия проводятся Администратором АИС периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и предназначены для осуществления контроля выполнения требований в области защиты информации в МДОУ «Ряжский детский сад № 1».

2.3. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн.

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:

2.4.1 по результатам расследования инцидента информационной безопасности;

2.4.2 по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.4.3 по решению заведующего МДОУ «Ряжский детский сад № 1».

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:

3.2.1 цели проведения контрольных мероприятий;

3.2.2 задачи проведения контрольных мероприятий,

3.2.3 объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4 состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5 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.

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает отчет, в котором указывается:

4.2.1 описание проведенных мероприятий по каждому из этапов;

4.2.2 перечень и описание выявленных нарушений;

4.2.3 рекомендации по устранению выявленных нарушений;

4.2.4 заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. отчет передается на рассмотрение заведующему МДОУ «Ряжский детский сад № 1».

4.4. Общая информации 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 персональных данных в МДОУ «Ряжский детский сад № 1» (приложение 2).

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Контрольные мероприятия проводятся ответственным за обеспечение безопасности обработки персональных данных в МДОУ «Ряжский детский сад № 1».

5.2. 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.

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

- Соответствие полномочий Пользователя правилам доступа.
- Соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн.
- Соблюдение Порядка доступа в помещения МДОУ «Ряжский детский сад № 1», где ведется обработка персональных данных.
- Порядок и условия применения средств защиты информации.
- Состояние учета машинных носителей персональных данных.
- 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 с штатным и нештатным функционированием средств защиты.
- Технические мероприятия, связанные с штатным и нештатным функционированием подсистем системы защиты информации.

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

ПЛАН

внутренних проверок контроля соответствия обработки персональных
данных требованиям к защите персональных данных

Мероприятие	Периодичность регулярных мероприятий	Периодичность плановых мероприятий	Исполнитель
Контроль соблюдения правил доступа к ПДн	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль соблюдения режима защиты	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль выполнения антивирусной политики	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль выполнения парольной политики	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль соблюдения режима защиты при подключении к сетям общего пользования	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн		Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль обновления ПО и единообразия применяемого ПО на всех элементах АИС	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных

_____ СПО			
Контроль обеспечения резервного копирования		Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз		Ежегодно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Поддержание в актуальном состоянии нормативно-организационных документов		Ежемесячно	Ответственный за организацию обработки ПДн в
Контроль запрета на использование беспроводных соединений	Еженедельно	Ежемесячно	

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

ПРОТОКОЛ № _____

проведения внутренних проверок контроля соответствия обработки
персональных данных требованиям к защите персональных данных в
МДОУ «Ряжский детский сад № 1»

Настоящий Протокол составлен в том, что «__» _____ 20__ г.

_____ (комиссией)
(должность, Ф.И.О. сотрудника)

проведена проверка _____
(тема проверки)

Проверка осуществлялась в соответствии с требованиями:

_____ (название документа)

В ходе проверки проверено:

Выявленные нарушения:

Меры по устранению нарушений:

Срок устранения нарушений: _____

Председатель комиссии:

фамилия и инициалы / подпись / должность

Члены комиссии:

фамилия и инициалы / подпись / должность

фамилия и инициалы / подпись / должность