ПРИЛОЖЕНИЕ № 3
УТВЕРЖДЕНО
приказом МБДОУ «Детский сад № 57 «Катюша»
от «13» 11 2017 г. № 195

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБДОУ «Детский сад № 57 «Катюша»

1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБДОУ «Детский сад № 57 «Катюша» (далее – Правила) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере защиты персональных данных, а также основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральным законом от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации», Трудовым кодексом Российской Федерации, постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 № 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» и другими нормативными правовыми актами.

3. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4. Контроль соответствия уровня защищенности персональных данных и соблюдения условий использования средств защиты информации, а также соблюдения требований законодательства Российской Федерации по обработке персональных данных в ИС МБДОУ «Детский сад № 57 «Катюша» (далее – Учреждение) проводится путем:

– проверки выполнения требований организационно-распорядительной документации по защите информации в Учреждении и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

– оценки уровня осведомленности и знаний работников Учреждения в области обработки и защиты персональных данных;

– оценки обоснованности и эффективности применяемых мер и средств защиты.

5. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении организовывается проведение периодических проверок условий обработки персональных данных (далее – проверки), которые разделяются на:

– плановые;

– внеплановые.

6. Плановые проверки проводятся ответственным за организацию обработки персональных данных в Учреждении, назначенным приказом заведующего Учреждением, в соответствии с утвержденным Планом проведения периодических проверок условий обработки персональных данных (далее – План), форма которого приведена в Приложении №1 к настоящим Правилам, и предназначены для осуществления контроля выполнения требований в области защиты информации в Учреждении.

7. Внеплановые проверки проводятся на основании решения комиссии по информационной безопасности, состав которой утверждается приказом заведующего Учреждением (далее – комиссия). Решение о проведении внеплановых проверок может быть принято в следующих случаях:

– на основании поступившего в Учреждение письменного заявления субъекта персональных данных о нарушениях правил обработки персональных данных;

– по результатам расследования инцидента информационной безопасности;

– по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

– по решению заведующего Учреждением.

8. Для проведения плановых проверок лицо, ответственное за организацию обработки персональных данных в Учреждении, разрабатывает Ежегодный план осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям.

Ежегодный план осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям включает следующие сведения по каждому из мероприятий:

– цели проведения проверки;

– задачи проведения проверки;

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

– состав участников, привлекаемых для проведения проверки;

– сроки и этапы проведения проверки.

Общий срок проверки не должен превышать пяти рабочих дней. При необходимости срок проведения проверки может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенной проверки.

9. Проведение внеплановой проверки организуется в течение трех рабочих дней с момента принятия заведующим Учреждением решения о необходимости ее проведения.

10. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены: .

– порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

– порядок и условия применения средств защиты информации;

– эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы;

– соответствие полномочий пользователей информационной системы Учреждения (далее – пользователи) правилам доступа;

– соблюдение пользователями требований инструкций по организации антивирусной и парольной политики;

– соблюдение администратором безопасности информационной системы инструкций и регламентов по обеспечению безопасности информации в Учреждении;

– соблюдение Порядка доступа в помещения Учреждения, в которых ведется обработка персональных данных;

– знание пользователями положений «Инструкции пользователя информационной системы МБДОУ «Детский сад № 57 «Катюша»;

– знание администратором безопасности информационной системы инструкций и регламентов по обеспечению безопасности информации в Учреждении;

– порядок и условия применения средств защиты информации.

– технические мероприятия, связанные с штатным и нештатным функционированием средств защиты;

– технические мероприятия, связанные с штатным и нештатным функционированием подсистем системы защиты информации;

– состояние учета машинных носителей персональных данных;

– соблюдение правил доступа к персональным данным;

– наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

– проведенные мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– осуществление мероприятий по обеспечению целостности персональных данных.

11. Ответственный за организацию обработки персональных данных в Учреждении, комиссия имеет право:

– запрашивать у сотрудников Учреждения информацию, необходимую для реализации полномочий;

– вносить заведующему Учреждением предложения по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

– вносить заведующему Учреждением предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

– вносить заведующему Учреждением предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

12. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в Учреждении или комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

13. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о ее проведении.

14. По итогам проведения проверок ответственный за организацию обработки персональных данных либо председатель комиссии разрабатывает 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.

Отчет передается на рассмотрение заведующему Учреждением.

15. Общая информации о проведенной проверке фиксируется в «Журнале по учету мероприятий по внутреннему контролю обработки персональных данных и обеспечения защиты персональных данных в ИС».

16. Результаты проведения внеплановых проверок заносятся в Протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в Учреждении (Приложение №2).

Приложение №1
к Правилам осуществления
внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБДОУ «Детский сад № 57 «Катюша»

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

Мероприятие	**Периодичность плановых мероприятий**	**Исполнитель**
Контроль соблюдения правил доступа к ПДн	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационной системе _____(_____) (подпись) (Фамилия И.О.)
Контроль соблюдения режима защиты	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационной системе _____(_____) (подпись) (Фамилия И.О.)
Контроль выполнения антивирусной политики	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационной системе _____(_____) (подпись) (Фамилия И.О.)
Контроль выполнения парольной политики	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационной системе _____(_____) (подпись) (Фамилия И.О.)
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационной системе _____(_____) (подпись) (Фамилия И.О.)
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационной системе _____(_____) (подпись) (Фамилия И.О.)
Контроль обновления ПО и единообразия применяемого ПО на всех элементах ИС	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационной системе _____(_____) (подпись) (Фамилия И.О.)
Контроль обеспечения резервного копирования	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационной системе _____(_____) (подпись) (Фамилия И.О.)

Мероприятие	Периодичность плановых мероприятий	Исполнитель
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	Ответственный за обеспечение безопасности персональных данных в информационной системе _____(_____) (подпись) (Фамилия И.О.)
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	Ответственный за организацию обработки персональных данных в информационной системе _____(_____) (подпись) (Фамилия И.О.)

Приложение №2
к Правилам осуществления
внутреннего контроля соответствия обработки персональных
данных требованиям к защите персональных данных в
МБДОУ «Детский сад № 57 «Катюша»

ПРОТОКОЛ № ____
проведения внутренних проверок контроля соответствия обработки
персональных данных требованиям к защите персональных данных в МБДОУ «Детский сад № 57 «Катюша»

Настоящий Протокол составлен в том, что «__»_____201_ 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