УТВЕРЖДАЮ
МАОУ «Заветинская НШ-ДС»
_____ О.Ю.Сенькина
«12» августа 2019г.

Документ подписан электронной подписью
Сенькина Ольга Юрьевна
директор
МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "ЗАВЕТИНСКАЯ НАЧАЛЬНАЯ ШКОЛА - ДЕТСКИЙ САД"
Серийный номер:
5695B24CA9DFD9E40D1E12D678009B85
Срок действия с 17.03.2023 до 09.06.2024

ПРАВИЛА
проведения внутреннего контроля

П. Фурмановка
2019 г.

1.

2. Общие положения

2.1 Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите информации (далее – Правила) в МАОУ «Заветинская НШ-ДС» (далее - Организация) определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПДн). Настоящие Правила разработаны в соответствии с:

– Федеральным законом от 27июля2006года №152-ФЗ «О персональных данных»;

– Постановлением Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказом ФСТЭК России №17 от 11 февраля 2013г. «Об утверждении Требований о защите информации, не содержащей государственную тайну, содержащейся в государственных информационных системах;

– Приказом ФСТЭК России №21 от 18 февраля 2012 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2.2 Внутренний контроль в Организации может осуществляться:

– администратором безопасности информации в государственных информационных системах Организации (далее –Администратор);

– ответственным за организацию обработки ПДн;

– Комиссией по обеспечению защиты персональных данных в Организации (далее – Комиссия);

– организациями, имеющими лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

2.3 Формы внутреннего контроля:

– текущий контроль, осуществляемый Администратором;

– периодический контроль, осуществляемый ответственным за организацию обработки ПДн;

– внеплановый контроль, осуществляемый Комиссией;

– комплексный контроль над выполнением установленных требований к защите персональных данных, организуемый Организацией и проводимый организацией, имеющей лицензию ФСТЭК на осуществление деятельности по технической защите конфиденциальной информации.

2.4 Проверки, проводимые в рамках внутреннего контроля, соответствия обработки персональных данных установленным требованиям в Организации (далее – проверки) могут быть плановые и внеплановые.

2.4.1 Плановые проверки проводятся на основании утвержденного Руководителем Организации ежегодного Плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям (Приложение №1).

2.4.2 Внеплановые проверки проводятся на основании решения Комиссии, которое может быть принято в следующих случаях:

– по результатам расследования инцидента информационной безопасности;

– по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

– выявления фактов незаконного разглашения (распространения) персональных данных.

Внеплановые проверки также проводятся на основании поступившего в Организацию письменного заявления субъекта ПДн о нарушениях правил обработки персональных данных. Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

3. Порядок проведения плановых и внеплановых проверок

3.1 Для проведения плановых проверок лицо, ответственное за организацию обработки ПДн, разрабатывает План осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям на текущий год (далее – План осуществления внутреннего контроля), который утверждается руководителем Организации.

3.2 Общий срок проведения проверки не должен превышать пятнадцати 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 проведенных проверок.

3.3 Плановые и внеплановые проверки проводятся при обязательном участии Администратора.

3.4 Администратор, не позднее чем за три рабочих дня до начала проведения проверки уведомляет всех руководителей структурных подразделений, в которых планируется проведение проверки, и направляет им для ознакомления План осуществления внутреннего контроля. При проведении внеплановых проверок уведомление не требуется.

3.5 В целях осуществления внутреннего контроля, в зависимости от его целей, могут выполняться следующие проверки:

– соответствие полномочий пользователя утвержденным правилам доступа;

– соблюдение пользователями требований Регламента по обеспечению информационной безопасности персональных данных в Организации;

– соблюдение Инструкции о порядке доступа сотрудников в помещения, предназначенные для обработки 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;

– соблюдение пользователями государственных информационных систем правил работы со съёмными носителями персональных данных;

– соблюдение правил работы со средствами криптографической защиты;

– соблюдение правил хранения и работы с бумажными носителями персональных данных.

3.6 При проведении проверки 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 персональных данных;

– состояние учета машинных носителей персональных данных;

– соблюдение правил доступа к персональным данным;

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

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

– осуществление мероприятий по обеспечению целостности персональных данных.

3.7 Проверки могут осуществляться как непосредственно на рабочих местах исполнителей, участвующих в обработке персональных данных, так и путем направления запросов и рассмотрения документов, необходимых для осуществления внутреннего контроля.

3.8 Проверка должна быть завершена не позднее чем через 15 рабочих дней с даты начала проверки.

4. Права и обязанности лиц, осуществляющих внутренний контроль

4.1 Права ответственного за организацию обработки ПДн, Администратора и Комиссии при проведении внутреннего контроля:

– запрашивать у руководителей структурных подразделенийинформацию и (или) документы, необходимые для осуществления внутреннего контроля;

– требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных.

– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

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

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

4.2 Лица, осуществляющие внутренний контроль, должны обеспечивать конфиденциальность ставших им известными в ходе проведения мероприятий внутреннего контроля персональных данных. В отношении персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

5. Результат проведения внутреннего контроля

5.1 По итогам проведения плановых и внеплановых контрольных мероприятий лицо (Комиссия) 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.

5.2 Отчет передается на рассмотрение руководителю Организации.

5.3 Результаты проведенных проверок оформляются в виде Акта внутреннего контроля (Приложение № 2), который подписывается членами Комиссии.

5.4 Мероприятия по контролю над соблюдением режима защиты персональных данных фиксируются в Журнале (Приложение 3).

5.5 О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, по мере необходимости председатель Комиссии докладывает руководителю Организации.

Приложение № 1
к Правилам проведения внутреннего контроля

ПЛАН
осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям

№	Тема проверки	Нормативный правовой документ предъявляющий требования	Срок проведения	Исполнитель

Приложение № 2
к Правилам проведения внутреннего контроля

Акт
внутреннего контроля соответствия обработки персональных данных в структурных подразделениях
_____ требованиям к защите персональных данных

Предмет контроля:
_____
_____
_____
_____
_____

Выявленные нарушения:
_____
_____
_____
_____
_____

Меры по устранению нарушений:
_____
_____
_____
_____
_____

Предложения комиссии:
_____
_____
_____
_____

Подписи членов комиссии:

_____ _____
(подпись)(фамилия, имя, отчество)

_____ _____
(подпись)(фамилия, имя, отчество)

_____ _____
(подпись)(фамилия, имя, отчество)

Приложение №3
к Правилам проведения внутреннего контроля

ЖУРНАЛ

учета мероприятий по контролю над соблюдением режима защиты персональных данных

№ п/п	Мероприятие	Дата	Исполнитель	Результат