Чернышова Наталия Николаевна

Подписан: Чернышова Наталия Николаевна
DN: OU=И.о. директора, O="МОАУ ""СОШ № 65""", CN=Чернышова Наталия Николаевна, E=65@orenschool.ru
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: место подписания
Дата: 2024.04.08 12:20:07+02'00'
Foxit PDF Reader Версия: 11.1.0

«УТВЕРЖДАЮ»
И.о. директора МОАУ «СОШ 65»
_____ Н.Н. Чернышова
Приказ № 229 от 01.09.2023 г.

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее -Правила контроля) в МОАУ «СОШ № 65» (далее - школа) 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 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» 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 Российской Федерации от 21 марта 2012 г. № 211.

1.3. Школа использует информационные системы персональных данных (далее -ИСПДн) для выполнения основных целей и задач обработки ПДн, указанных в пункте 2 Положения по обработке и защите персональных данных.

1.4. Пользователями ИСПДн (далее - Пользователь) являются сотрудники школы, 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 школы проводятся в следующих целях:

- проверка выполнения требований организационно-распорядительной документации по защите информации в школе и действующего законодательства Российской Федерации в области обработки и защиты ПДн;
- оценка уровня осведомленности и знаний сотрудников школы в области обработки и защиты ПДн;
- оценка обоснованности и эффективности применяемых мер и средств защиты ПДн.

2. Тематика внутреннего контроля

2.1. Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

Проверки соответствия обработки ПДн установленным требованиям в Школе 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 школы) проведения контрольных мероприятий (далее - План) и предназначены для осуществления контроля выполнения требований в области защиты информации в школе.

2.3. Плановые контрольные мероприятия периодически проводятся постоянной комиссией в соответствии с утвержденным Планом и направлены на постоянное совершенствование системы защиты ПДн ИСПДн школы.

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 школы.

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 руководителя школы.

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 ПДн требованиям к защите ПДн в школе (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 ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы ИС и ответственные за обеспечение безопасности ПДн информационных систем ПДн.

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. 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 школе;
- соблюдения порядка доступа сотрудников в помещения школы, 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 школе;
- 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

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	Ответственное лицо
Контроль соблюдения режима защиты	Еженедельно	Ежемесячно	Ответственное лицо
Контроль выполнения антивирусной политики	Еженедельно	Ежемесячно	Ответственное лицо
Контроль соблюдения правил доступа к ПДн	Еженедельно	Ежемесячно	Ответственное лицо
Контроль выполнения парольной политики	Еженедельно	Ежемесячно	Ответственное лицо
Контроль соблюдения режима защиты при подключении к сетям общего пользованиями (или) международного обмена	Еженедельно	Ежемесячно	Ответственное лицо
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Еженедельно	Ежемесячно	Ответственное лицо
Контроль обновления ПО и единообразия, применяемого ПО на всех элементах ИС	Еженедельно	Ежемесячно	Ответственное лицо
Контроль обеспечения резервного копирования	Еженедельно	Ежемесячно	Ответственное лицо
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Еженедельно	Ежемесячно	Ответственное лицо
Поддержание в актуальном состоянии нормативно-организационных документов	Еженедельно	Ежемесячно	Ответственное лицо
Контроль запрета на использование беспроводных соединений	Еженедельно	Ежемесячно	Ответственное лицо

Приложение 2

Ж У Р Н А Л
учета событий информационной безопасности
в МОАУ «СОШ № 65»

№ п/п	Дата события	Основания возникновения события	Описание события (мероприятия)	Характеристика события	Ф.И.О. субъекта	Должность, ФИО и подпись ответственного за ведение журнала	Приме-чание

Приложение 3

ПРОТОКОЛ №
проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

Настоящий Протокол составлен о том, что «___»_____ 20____г. проведена проверка комиссией в составе:

1._____
(должность, Ф.И.О.)
2._____
(должность, Ф.И.О.)
3._____
(должность, Ф.И.О.)

Проверка осуществлялась в соответствии с требованиями:
_____
_____

В ходе проверки проверено:_____
_____
_____

Выявленные нарушения: _____
_____
_____

Меры по устранению нарушений:_____
_____
_____

Срок устранения нарушений:_____

1._____
(должность, Ф.И.О.)
2._____
(должность, Ф.И.О.)
3._____

(должность, Ф.И.О.)