Муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа № 24»

Принято
на общем собрании
трудового коллектива
протокол № 3
« 27 » августа 2021 г.

Утверждаю
Директор МБОУ «СОШ № 24»
Приказ № 69/17-ОД
« 31 » августа 2021 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) в МБОУ «СОШ №24» (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.

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

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1. 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) 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 директора Школы.

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности ПДн, 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 5 (пяти) рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на 10 (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).
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 директору 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 защите ПДн в школе (Приложение 3).

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 3 (три) рабочих дня до начала проведения контрольных мероприятий уведомляет сотрудников, в отношении которых должна быть проведена проверка, 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 администратором ИСПДн инструкций и регламентов по обеспечению безопасности информации в Школе;
- соблюдения порядка доступа сотрудников в помещения Школы, где ведется обработка ПДн;
- знания Пользователями положений инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций;

- знание администратором ИСПДн инструкций и регламентов по обеспечению безопасности информации в Школе;
- порядок и условия применения СЗИ;
- 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 СЗИ.

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

Приложение 2

ЖУРНАЛ
учета событий информационной безопасности

Журнал начат « »	_____ 20__ г.	Журнал завершен «	__»_____	20 г.
Должность		Должность		
/	_____ /	/		/

№ п/п	Дата события	Основания возникновения события	Описание события (мероприятия)	Характеристика события	(ФИО, субъекта)	Должность, ФИО и подпись ответственного за ведение журнала	Примечание

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)
(должность, Ф.И.О. сотрудника)

_____

_____
(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)