



**Муниципальное бюджетное общеобразовательное учреждение «Средняя общеобразовательная школа № 2»
(МБОУ «Средняя общеобразовательная школа № 2»)
ул. Анохина, дом 110, г. Чита, Забайкальский край, РФ, 672000
Тел.: +7 (3022) 35-15-33, E-mail: shs_chit_2@chita.e-zab.ru**

СОГЛАСОВАНО:

Председатель Первичной профсоюзной
организации МБОУ «СОШ № 2»
И.А.Климова

УТВЕРЖДЕНО

Приказом директора МБОУ «СОШ № 2» от
02.05.2024 № 60/4-О/Д

**ПРАВИЛА
осуществления внутреннего аудита
соответствия обработки персональных данных
в МБОУ «Средняя общеобразовательная школа № 2»**

г. Чита, 2024 г.

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила контроля) в Муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа № 2» (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», утверждённых 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 порядке обработки персональных данных в МБОУ «Средняя общеобразовательная школа № 2».

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 утверждённым 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 утверждённым Планом и направлены на постоянное совершенствование системы защиты ПДн ИСПДн школы.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создаётся на период проведения мероприятий).

Решение о проведении внеплановых контрольных мероприятий и создании 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. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлён, но не более чем на десять рабочих дней, соответствующие изменения отображаются в отчёте, выполняемом по результатам проведённых контрольных мероприятий.

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируются 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 отчёт, в котором указывается:

- описание проведённых мероприятий по каждому из этапов;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений;
- заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. Отчёт передаётся на рассмотрение руководителя школы.

4.4. Общая информация о проведённом 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

*к Правилам осуществления внутреннего контроля соответствия обработки персональным
данным требованиям к защите персональных данных*

Мероприятие	Периодичность выполнения	Результат
<i>Организационные мероприятия</i>		
Создание постоянно действующей комиссии по защите информации	Разовое	Приказ о комиссии по информационной безопасности
Назначение ответственных за безопасность ПДн	Разовое	Приказ о подразделении по защите персональных данных или Приказ о назначении ответственных лиц в информационных системах
Определение перечня ИСПДн	Разовое	Перечень ИСПДн
Определение обрабатываемых ПДн и объектов защиты, целесообразность обработки ПДн, правовые основания для обработки ПДн	Разовое	Перечень защищаемых ресурсов
Определение круга лиц, участвующих в обработке ПДн	Разовое	Перечень лиц, имеющих доступ к ИСПДн
Определение ответственности лиц участвующих в обработке	Разовое	Обязательство о неразглашении ПДн
Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	Разовое	Разрешительная система доступа
Классификация всех выявленных ИСПДн	Разовое	Акты классификации
Принятие документов регламентирующих обработку ПД	Разовое	Организационные распорядительные документы по ПДн, Положение о защите ПДн в ИСПДн
Подача уведомления об обработке персональных данных		Направить уведомления об обработке персональных данных в соответствующий территориальный орган Роскомнадзора по месту регистрации оператора
Выбор помещений для установки аппаратных средств ИСПДн в помещениях, с целью исключения НСД лиц, не допущенных к обработке ПДн	Разовое	
Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн.	Разовое	
Организация порядка резервного копирования защищаемой информации на	Разовое	

Мероприятие	Периодичность выполнения	Результат
твердые носители		
Организация порядка восстановления работоспособности технических средств, ПО, баз данных с подсистем СЗПДн	Разовое	
Создание журнала учета обращений субъектов ПДн	Разовое	Журнал учета обращений субъектов персональных данных о соблюдении их законных прав, при обработке персональных данных в ИСПДн
Анализ актуальности угроз безопасности персональным данным (УБПДн)	Разовое	Модель угроз
Организация информирования и обучения сотрудников о порядке обработки ПДн	Разовое	
Разработка должностных инструкций о порядке обработки ПДн и обеспечении введенного режима защиты	Разовое	Инструкция пользователя ИСПДн
Разработка должностных инструкций ответственных за обеспечение безопасности ПДн	Разовое	Инструкция безопасности информации ИСПДн
Разработка положения о внесении изменения в штатное программное обеспечение элементов ИСПДн	Разовое	Положение о внесении изменения в штатное программное обеспечение элементов ИСПДн
Организация перечня по учету технических средств и средств защиты, а так же документации к ним	Разовое	Журналы учета технических средств и средств защиты, а так же документации к ним
<i>Физические мероприятия</i>		
Установление контролируемой зоны вокруг ИСПДн	Разовое	
Организация постов охраны для пропуска в контролируемую зону	Разовое	
Установка жалюзи, штор на окнах или другие меры, исключающие несанкционированный доступ к ПД снаружи здания	Разовое	
<i>Технические (аппаратные и программные) мероприятия</i>		
Внедрение единого хранилища зарегистрированных действий пользователей с ПДн	Разовое	
Внедрение специальной подсистемы управления доступом, регистрации и учета	Разовое	
Внедрение межсетевое экранирования	Разовое	
Внедрение подсистемы анализа защищенности	Разовое	

Мероприятие	Периодичность выполнения	Результат
Внедрение подсистемы обнаружения вторжений	Разовое	
Внедрение криптографической защиты	Разовое	
Внедрение антивирусной защиты	Разовое	
<i>Контролирующие мероприятия</i>		
Создание журнала внутренних проверок и поддержание его в актуальном состоянии	Разовое	Ведение журнала
Контроль над соблюдением режима обработки ПДн	Еженедельно	
Контроль над соблюдением режима защиты	Еженедельно	
Контроль над выполнением антивирусной защиты	Еженедельно	
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	
Контроль за обеспечением резервного копирования	Ежемесячно	
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	
Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями.	Ежемесячно	

к Правилам осуществления внутреннего контроля соответствия обработки
персональным данным
требованиям к защите персональных данных

Ж У Р Н А Л

учета событий информационной безопасности

Журнал начат	20 г.	Журнал завершен		20 г.
Должность		Должность		
/		/	/	/

№ п/п	Дата событ ия	Основания возникнове ния события	Описание события (мероприя тия)	Характерист ика события	(ФИО, субъекта)	Должность, ФИО и подпись ответственного за ведение журнала	Примечание

Приложение 3

*к Правилам осуществления внутреннего контроля соответствия обработки
персональным
данным требованиям к защите персональных
данных*

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

Настоящий Протокол составлен о том, что « »__20 г. проведена проверка_____

_(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: