

ПРИНЯТО
на заседании педагогического совета
Протокол № 8 от 30.05.2025



УТВЕРЖДАЮ
Директор МБОУ СОШ
с. Большой Труев
Д.Р. Хусаинова
Приказ № 43/1 от 04.06.2025

ПОЛОЖЕНИЕ
о внутреннем контроле и (или) аудите соответствия обработки
персональных данных в МБОУ СОШ с. Большой Труев требованиям
законодательства в сфере обработки персональных данных

1. Общие положения

1.1. Настоящее Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в МБОУ СОШ с. Большой Труев требованиям законодательства в сфере обработки персональных данных (далее — Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Положение определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных в МБОУ СОШ с. Большой Труев (далее — образовательная организация) требованиям к защите персональных данных, установленным законодательством Российской Федерации.

1.3. Исполнение Положения обязательно для всех работников образовательной организации, осуществляющих обработку персональных данных, как без использования средств автоматизации, так и в информационных системах обработки персональных данных.

1.4. В Положении используются основные понятия в значениях, определенных в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Внутренний контроль соответствия обработки персональных данных — контроль соответствия обработки персональных данных в образовательной организации требованиям законодательства в сфере обработки персональных данных, проводимый силами образовательной организации в соответствии с Положением и другими локальными нормативными актами организации.

Внутренний аудит соответствия обработки персональных данных — контроль соответствия обработки персональных данных в образовательной организации требованиям законодательства в сфере обработки персональных данных, проводимый специализированными организациями, привлекаемыми образовательной организацией по договорам оказания услуг в соответствии с Положением и другими локальными нормативными актами организации.

2. Порядок проведения внутреннего контроля

2.1. Внутренний контроль соответствия обработки персональных данных осуществляется комиссией по плану мероприятий внутреннего контроля, утверждаемому ежегодно директором образовательной организации.

2.2. Мероприятия внутреннего контроля могут быть внеплановыми по решению комиссии, если есть фактические основания полагать, что процедура обработки персональных данных в образовательной организации не соответствует требованиям законодательства Российской Федерации.

2.3. Состав комиссии утверждается директором образовательной организации.

2.4. Мероприятия внутреннего контроля 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.

2.5. При проведении мероприятия внутреннего контроля 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;
- 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.

2.6. Комиссия при проведении внутреннего контроля имеет право:

- запрашивать у работников, осуществляющих обработку персональных данных, информацию и (или) документы, необходимые для осуществления внутреннего контроля;
- требовать у ответственных за обработку персональных данных 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 предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке в образовательной организации;
- вносить предложения о привлечении к дисциплинарной ответственности работников, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

2.7. В отношении персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

2.8. Мероприятие внутреннего контроля не может длиться больше 10 рабочих дней. Срок мероприятия может быть продлен распорядительным актом руководителя образовательной организации при наличии оснований, не позволяющих закончить контрольное мероприятие за 10 рабочих дней. ▀

3. Оформление итогов внутреннего контроля

3.1. Результаты внутреннего контроля соответствия обработки персональных данных оформляются комиссией в виде акта внутреннего контроля. Члены комиссии обязаны составлять докладные записки по итогам контрольных мероприятий, если это предусматривает план мероприятий внутреннего контроля или распорядительный акт директора образовательной организации.

3.2. Акт внутреннего контроля подписывается всеми членами комиссии.

3.3. Выявленные в ходе внутреннего контроля нарушения фиксируются в акте внутреннего контроля с предложениями мероприятий по устранению нарушений и сроков их выполнения.

3.4. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, по мере необходимости комиссия докладывает на очередном совещании при директоре образовательной организации, если иное не установлено распорядительным актом директора образовательной организации.

3.5. Акты внутреннего контроля, докладные записки по итогам контрольных мероприятий хранятся в запирающемся шкафу в кабинете директора образовательной организации.

4. Порядок проведения внутреннего аудита

4.1. Внутренний аудит соответствия обработки персональных данных проводится в случаях, когда образовательная организация не может объективно оценить соответствие обработки персональных данных в образовательной организации требованиям законодательства в сфере обработки персональных данных.

4.2. Внутренний аудит организуется на основании распорядительного акта директора образовательной организации.

4.3 Внутренний аудит проводит организация, которая в соответствии со своими учредительными документами занимается оценкой рисков в обработке персональных данных и возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4.4. На время проведения внутреннего аудита директор образовательной организации назначает ответственного, который должен взаимодействовать с организацией, проводящей аудит (далее — аудитор).

4.5. Ответственный обязан:

- обеспечить аудитора всей необходимой информацией;
- организовать условия для работы;
- оказывать помощь при возникновении трудностей;
- контролировать работу аудитора;
- принимать все отчеты аудитора и доводить их до сведения директора образовательной организации.

4.6. Действия и обязанности аудитора определяются заключенным договором оказания услуг по проведению внутреннего аудита.

4.7. Документы внутреннего аудита, в том числе итоговые отчеты, хранятся в запирающемся шкафу в кабинете директора образовательной организации.

Приложение 1 к Положению о внутреннем контроле и
(или) аудите соответствия обработки персональных данных
в МБОУ СОШ с. Большой Труев требованиям
законодательства в сфере обработки персональных данных

План внутреннего контроля и (или) соответствия обработки
и защиты персональных данных

№ п/п	Мероприятие	Периодичность	Исполнитель	Отметка об исполнении
1.	Контроль компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов)	Постоянно	Ответственный за обеспечение безопасности персональных данных в информационных системах	Еженедельно. Журнал учета работ в ИС
2.	Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных	1 раз в 3 года	Ответственный за обеспечение безопасности персональных данных в ИСПДн	Акт оценки эффективности мер по обеспечению безопасности персональных данных
3.	Организация анализа и пересмотра имеющихся угроз безопасности ЗИ, а также предсказание появления новых угроз	Ежегодно	Ответственный за обеспечение безопасности персональных данных в информационных системах	Журнал учета работ в ИС

4.	Проведение внутренних проверок на предмет соответствия обработки персональных данных требованиям к защите персональных данных	Ежегодно	Ответственный за организацию обработки персональных данных, либо комиссия	Журнал учета работ в ИС, акт внутренней проверки
----	---	----------	---	--

5.	Поддержание в актуальном состоянии документа «Список лиц, доступ которых к защищаемой информации необходим для выполнения служебных (трудовых) обязанностей»	Ежемесячно	Ответственный за организацию обработки персональных данных	Журнал учета работ в ИС
6.	Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИС	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационных системах	Журнал учета работ в ИС
7.	Проведение мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИС и по реагированию на компьютерные инциденты в них	Постоянно	Ответственный за обеспечение безопасности персональных данных в информационных системах	Журнал учета работ в ИС

8.	Контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационных системах	Журнал учета работ в ИС
9.	Контроль наличия и местонахождения машинных носителей информации.	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационных системах	Журнал учета работ в ИС
10.	Контроль за обеспечением резервного копирования	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационных системах	Журнал учета работ в ИС

11.	Контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации	Ежемесячно	Ответственный за обеспечение безопасности персональных данных в информационных системах	Журнал учёта средств защиты информации, эксплуатационной и технической документации к ним
-----	---	------------	---	---

12.	Контроль за соблюдением режима безопасности помещений в которых осуществляется обработка персональных данных	Ежеквартально	Ответственный за организацию обработки персональных данных	Журнал учета ключей от сейфов и помещений
13.	Контроль за соблюдением режима безопасности помещений, в которых размещена информационная система	Ежеквартально	Ответственный за организацию обработки персональных данных	Журнал учета работ в ИС
14.	Контроль сохранности носителей защищаемой информации	Ежеквартально	Ответственный за обеспечение безопасности персональных данных в информационных системах	Журнал учета съемных носителей информации
15.	Поддержание в актуальном состоянии организационно-распорядительных документов	Ежеквартально	Ответственный за организацию обработки персональных данных	Журнал учета работ в ИС
16.	Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Ответственный за обеспечение безопасности персональных данных информационных системах	Журнал учета работ в ИС