СОГЛАСОВАНО:
Председатель Профсоюзного комитета
_____
Протокол № 1 от
«30» 08 2022

ПРИНЯТО:
педагогическим советом
Протокол № 3 от
«30» 08 2022

УТВЕРЖДАЮ:
Директор школы:
В.Н. Зайцев
_____
Приказ от «30» 08 2022
№114

Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в МБОУ «Шебалинская СОШ им. В.И. Фомичева» 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 «Шебалинская СОШ им. В.И. Фомичёва» 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 «Шебалинская СОШ им. В.И. Фомичёва» (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 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 деятельности комиссии 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. 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.

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

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

3. Порядок проведения внутренних проверок

3.1. Порядок проведения контроля установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

В ходе проведения проверки необходимо:

3.1.1. Проверить соответствие версий общесистемного, прикладного и специального программного обеспечения, включая программное обеспечение средств защиты информации

3.1.2. Проверить наличие отметок в эксплуатационной документации (формуляр, паспорт) об установке (применении) обновлений.

3.2. Порядок проведения контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

3.2.1 Проверить работоспособность (неотключение) программного обеспечения и средств защиты информации.

3.2.2 Проверить правильность функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации.

3.2.3 Проверить соответствие настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации.

3.2.4 В случае возникновения необходимости восстановить работоспособность, правильное функционирование, а также параметры настройки программного обеспечения и средств защиты информации, в том числе с использованием резервных копий и (или) дистрибутивов.

3.3 Порядок проведения контроля состава технических средств, программного обеспечения и средств защиты информации.

3.3.1 Проверить соответствие состава программного обеспечения, технических средств и средств защиты информации приведенному в локальных документах образовательной организации и эксплуатационной документации.

3.3.2 Исключить из состава информационной системы несанкционированно установленные (удаленные) технические средства, программное обеспечение и средства защиты информации.

3.3.3 Проверить выполнение условий и сроков действия сертификатов соответствия на средства защиты информации.

3.3.4 В случае возникновения необходимости принять меры, направленные на устранения выявленных недостатков.

3.4 Порядок проведения контроля правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИСПДн .

3.4.1 Проверить соблюдение пользователями и ответственными лицами правил генерации и смены паролей пользователей.

3.4.2 Проверить соответствие заведенных и удаленных учетных записей пользователей локальным документам образовательной организации.

3.4.3 Осуществить проверку реализации правил разграничения доступа и полномочий пользователей в соответствии с утвержденной матрицей доступа.

3.4.4 Провести контроль наличия документов, подтверждающих разрешение изменения учетных записей пользователей, их параметров, правил разграничения доступа, установленных полномочий пользователей.

3.4.5 В случае возникновения необходимости принять меры, направленные на устранения выявленных недостатков.

3.5 Порядок проведения проверки соблюдения режима защиты персональных данных при их обработке в ИСПДн.

3.5.1 Определить соблюдают ли работники, участвующие в процессе обработки персональных данных в информационной системе персональных данных, принятые меры по обеспечению безопасности персональных данных.

3.5.2 Произвести контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена.

3.5.3 Осуществить проверку наличия машинных носителей персональных данных.

3.5.4 Проверить наличие и ведение журналов, используемых для контроля (анализа) защищенности персональных данных.

3.5.5 Произвести контроль над выполнением резервного копирования и архивирования информации ограниченного доступа.

3.6 Порядок проведения анализа и пересмотра существующих мер по обеспечению безопасности персональных данных в ИСПДн.

3.6.1 Определить изменения в базовой конфигурации информационной системы, проверить наличие данных о внесении изменений в документацию на систему защиты информации информационной системы персональных данных.

3.6.2 Провести анализ произведенных изменений на предмет возникновения дополнительных угроз безопасности персональных данных в информационной системе персональных данных.

3.6.3 В случае выявления новых источников угроз провести уточнение и дополнение модели угроз безопасности.

3.6.4 Провести соотношение выявленных угроз информационной безопасности с реализованными мерами по обеспечению безопасности персональных данных, в случае необходимости применить дополнительные меры по обеспечению безопасности.

3.6.5 По результатам анализа изменённой модели угроз и выбора необходимых дополнительных мер по обеспечению безопасности – принять решение об обновлении либо модернизации системы защиты информации.

3.6.6 Принять решение о необходимости переаттестации информационной системы персональных данных или проведении дополнительных аттестационных испытаний.

3.7 Порядок проведения проверки наличия и актуальности внутренней нормативной документации по защите персональных данных.

3.7.1 Проверить наличие в образовательной организации и соответствие действующему законодательству РФ необходимой внутренней нормативной базы, регулирующей вопросы защиты персональных данных.

3.7.2 Проверить наличие доказательств ознакомления работников образовательной организации с внутренними нормативными документами (приказами, инструкциями и т.п.), регулирующими вопросы защиты персональных данных в образовательной организации.

3.7.3 Принять решение о необходимости актуализации внутренней нормативной базы.

4. Оформление итогов внутреннего контроля

4.1. Результаты внутреннего контроля соответствия обработки персональных данных оформляются комиссий в виде акта внутреннего контроля, составленного по форме согласно Приложению 1 к Положению, результаты проверок фиксируются в журнале регистрации проверок (приложение 2) и журнале выявленных нарушений (приложение 3). Члены комиссии обязаны составлять докладные записки по итогам контрольных мероприятий, если это предусматривает план мероприятий внутреннего контроля или распорядительный акт директора образовательной организации.

4.2. 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.

4.4. 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.

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

5. Порядок проведения внутреннего аудита

5.1. 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.

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

5.3 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».

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

5.5. 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.

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

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

Приложение № 1
к Положению о внутреннем контроле и (или) аудите
соответствия обработки персональных данных

Муниципальное бюджетное общеобразовательное учреждение «Шебалинская средняя общеобразовательная школа им. В.И. Фомичёва»

Утверждаю
Ответственный за организацию обработки персональных данных в МБОУ «Шебалинская СОШ им. В.И. Фомичёва»

_____ (ФИО)
«____»_____20___г.

Акт
внутреннего контроля и (или) аудита
соответствия обработки персональных данных
в МБОУ «Шебалинская СОШ им. В.И. Фомичева»
требованиям законодательства в сфере обработки персональных данных

«___»_____20__г. №____

Комиссия МБОУ «Шебалинская СОШ им. В.И. Фомичева» в составе:

1)_____ _____
(должность) (ФИО)

2)_____ _____
(должность) (ФИО)

3)_____ _____
(должность) (ФИО)

4)_____ _____
(должность) (ФИО)

провела внутренний контроль соответствия обработки персональных данных в МБОУ «Шебалинская СОШ им. В.И. Фомичева» требованиям законодательства в сфере обработки персональных данных в соответствии с планом внутреннего контроля на _____учебный год, утвержденным приказом директора МБОУ «Шебалинская СОШ им. В.И. Фомичева» от _____ №_____.

В ходе контрольных мероприятий проверены:

_____

Выявленные нарушения:

_____

Меры по устранению нарушений:

_____

Срок устранения нарушений: _____
Ответственный за исполнение: _____
Подписи членов комиссии:

_____ _____ _____
(подпись) (ФИО)

_____ _____ _____
(подпись) (ФИО)

_____ _____ _____
(подпись) (ФИО)

_____ _____ _____

(подпись) (ФИО)

Приложение 2
к Положению о внутреннем контроле и (или) аудите
соответствия обработки персональных данных

ЖУРНАЛ
регистрации проверок в сфере защиты персональных данных

Начат «___» _____ 20__ г.
Окончен «___» _____ 20__ г.

№ п/п	Дата выявления нарушения	Подразделение, где выявлено нарушение и допустившее нарушение лицо (ФИО, должность)	Кем и при каких обстоятельствах выявлено нарушение (жалоба, плановая проверка и т.д.)	Содержание нарушения	Требования, каких нормативных документов нарушены	Корректирующие и предупреждающие действия по устранению нарушения и предотвращению нарушения в дальнейшем	Ответственное за устранение лицо выявленного нарушения лицо (ФИО, должность и его подпись)	Срок устранения нарушения	Отметка о контроле за выполнением (дата, ФИО и должность проверяющего)