ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ МЕСТНОЙ АДМИНИСТРАЦИИ
МУНИЦИПАЛЬНОЕ КАЗЁННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 21
с УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ ОТДЕЛЬНЫХ ПРЕДМЕТОВ г. о.НАЛЬЧИК

360009, КБР, г. о.Нальчик, ул. Тимирязева, 7 Телефон: (8662) 91-16-19, 91-17-29 e-mail: school_iac @mail.ru
ОГРН 1020700750333 ИНН 0711038298 КПП 072601001 Сайт: http://www.школа21нальчик.рф

ПРИКАЗ

№ 01-10-279 26 августа 2025г.

г. о.Нальчик

О возложении персональной ответственности на сотрудников по защите персональных данных

В целях обеспечения защиты информации, руководствуясь Федеральным законом от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Назначить ответственным лицом за организацию мероприятий по защите персональных данных обучающихся - зам директора по УВР Алехину И.А., сотрудников - Соспинову Э.В.
2. Назначить ответственным за соблюдение норм антивирусной и парольной защиты на инженера-электроника Саракуева А.Х. и Щекина Н.Ю
3. Ответственным лицам в части персональной компетенции каждого для обеспечения защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, предоставления, распространения и иных неправомерных действий, а также соблюдения прав граждан на неразглашение их персональных данных, принимать следующие меры:
   - ❖ исключить возможность несанкционированного доступа к информации;
   - ❖ своевременно обнаруживать факты несанкционированного доступа к информации;
   - ❖ предупреждать возможность неблагоприятных последствий нарушения порядка доступа к информации;
   - ❖ не допускать воздействие на технические средства обработки информации, в результате которого нарушается их функционирование;
   - ❖ использовать все возможности незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
   - ❖ обеспечивать постоянный контроль за уровнем защищенности информации
4. Продолжить использование:

4.1. Формы обязательства о неразглашении персональных данных, согласно приложению 1 к настоящему приказу.

4.2. Перечня сведений конфиденциального характера согласно приложению 2 к настоящему приказу.

4.3. Порядка доступа сотрудников в помещения, в которых ведется обработка конфиденциальной информации, в т.ч. ПДн согласно приложению 3 к настоящему приказу.

5. Руководствоваться инструкциями и правилаи по защите информации:

5.1. инструкцией ответственного за организацию обработки ПДн согласно приложению 4 к настоящему приказу;

5.2. инструкцией по организации антивирусной защиты, согласно приложению 5 к настоящему приказу;

5.3. правилами осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, согласно приложению 6 к настоящему приказу;

6. Соспиновой Э.В., специалисту по кадрам, ознакомить сотрудников с приказом под подпись.

7. Контроль исполнения настоящего приказа оставляю за собой.

Директор школы _____/З.М.Казакова

С приказом ознакомлены:

Приложение 1
к приказу от 23. 08.2024 № 01-10-215

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных

*Я,*_____
(ФИО должность)
_____, предупрежден(а) о том, что на период исполнения должностных обязанностей в МКОУ «СОШ №21» мне будет предоставлен допуск к информации, содержащей персональные данные и конфиденциальной информации.

При работе с персональными данными обязуюсь:

- ❖ не разглашать сведения, содержащие персональные данные и конфиденциальную информацию, которые мне были доверены или станут известны при выполнении служебных обязанностей;
- ❖ не передавать (в любом виде) конфиденциальную информацию и сведения, содержащие персональные данные, третьим лицам, не имеющим доступа к этим сведениям;
- ❖ выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальной информации и персональных данных;
- ❖ в случае попытки посторонних лиц получить от меня конфиденциальную информацию и сведения, содержащие персональные данные, немедленно сообщить об этом непосредственному начальнику или (в случае его отсутствия) вышестоящему руководителю;
- ❖ не использовать конфиденциальную информацию и сведения, содержащие персональные данные, с целью получения выгоды;
- ❖ при прекращении моего права на допуск к конфиденциальной информации и сведениям, содержащим персональные данные (перевод на должность, не предусматривающую доступ к конфиденциальной информации и сведениям, содержащим персональные данные, расторжения служебного контракта

(контракта) или трудового договора), прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, все документы и иные материальные носители информации со сведениями, содержащими служебную информацию ограниченного распространения, и другие документы, которые находились в моем распоряжении в связи с выполнением мною должностных обязанностей на время работы, сдать непосредственному начальнику.

Мне известно, что нарушение требований, приведенных в этих документах, может повлечь административную, гражданско-правовую и иную ответственность в соответствии с действующим законодательством Российской Федерации.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных, или их утраты я понесу дисциплинарную, административную ответственность в соответствии со ст. 90 Трудового кодекса Российской Федерации, а также ст. 13.14 Кодекса Российской Федерации об административных правонарушениях.

«___»_____г. _____ _____

(число, месяц, год) (подпись) (ФИО)

Приложение 2
к приказу от 23. 08.2024 № 01-10-215

ПЕРЕЧЕНЬ сведений конфиденциального характера

№ п/ п	Содержание сведений, отнесённых к разряду ограниченного распространения	Нормативно-правовой акт, определяющий основание отнесения служебной информации к разряду ограниченного распространения
Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях		
1	Сведения, содержащие персональные данные, обрабатываемые вМКОУ «СОШ №21», в рамках реализации и выполнения работ, предусмотренных нормативными правовыми актами Российской Федерации: Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» и в соответствии с постановлением Правительства Российской Федерации от 29.11.2021 № 2085:	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных» квалификация, сведения об ученой степени)
	❖ фамилия, имя, отчество; ❖ число, месяц, год рождения; ❖ вид, серия, номер документа, удостоверяющего личность, дата выдачи, наименование органа его выдавшего; ❖ пол; ❖ идентификационный номер налогоплательщика;	

	❖ сведения о гражданстве; ❖ адрес места жительства (адрес регистрации); ❖ номер контактного телефона; ❖ электронный адрес в сети «Интернет»; ❖ реквизиты страхового свидетельства государственного пенсионного страхования; ❖ сведения об образовании (уровень профессионального образования, ❖ сведения о трудовой деятельности (место работы, должность, педагогический стаж, предметная специализация); ❖ номер расчетного счета; ❖ сведения о состоянии здоровья (рекомендации психолого-медикопедагогической комиссии, справка, подтверждающей факт установления инвалидности).	

Приложение 3
к приказу от 23. 08.2024 № 01-10-215

Порядок доступа сотрудников в помещения, в которых ведется обработка конфиденциальной информации, в т. ч. персональных данных

1 Общие положения

1.1 Настоящий Порядок доступа сотрудников в помещения, в которых ведется обработка конфиденциальной информации, в т. ч. персональных данных в МКОУ «СОШ №21» определяет правила доступа сотрудников в помещения, в которых ведется обработка конфиденциальной информации, включая персональные данные, в том числе с использованием средств криптографической защиты информации (далее – СКЗИ) на средствах вычислительной техники (далее – СВТ), с использованием и без использования средств автоматизации в рабочее и нерабочее время, а также в нештатных ситуациях.

1.2 Настоящий Порядок обязателен для применения и исполнения администрацией и всеми сотрудниками, осуществляющими обработку конфиденциальной информации, включая персональные данные, в том числе с использованием и без использования средств автоматизации, с использованием СКЗИ на СВТ.

1.3 Ответственность за соблюдение требований настоящего Порядка несут все сотрудники МКОУ «СОШ №21», участвующие в обработке конфиденциальной информации, в т.ч. персональных данных,

1.4 Контроль соблюдения требований настоящего Порядка обеспечивают должностные лица МКОУ «СОШ №21».

2 Требования к помещениям, в которых ведется обработка конфиденциальной информации, в т. ч. персональных данных, с использованием СКЗИ на СВТ

2.1 Бесконтрольный доступ посторонних лиц в помещения, в которых используются СКЗИ должен быть исключён.

2.2 Все помещения, в которых используются СКЗИ должны быть оборудованы входными дверьми с замками, а также же опечатывающими устройствами или техническими устройствами, сигнализирующими о несанкционированном вскрытии

помещений, с целью обеспечить постоянное закрытие помещений и их открытия только для санкционированного прохода.

Особое внимание при оснащении помещений техническими средствами, препятствующими осуществлению несанкционированного проникновения или пребывания, рекомендуется уделить на наличие исправного резервного источника питания на случай отключения промышленной электросети.

3 Порядок доступа в помещения, в которых ведется обработка конфиденциальной информации, в т.ч. персональных данных в рабочее, нерабочее время, в нештатных ситуациях

3.1 Директором МКОУ «СОШ №21» утверждается перечень мест обработки и хранения конфиденциальной информации, в т.ч. персональных данных, и ответственных должностных лиц.

В соответствии с данным перечнем организовывается контроль доступа сотрудников и посетителей в указанные помещения.

3.2 Доступ сотрудников МКОУ «СОШ №21» в помещения, в которых осуществляется обработка конфиденциальной информации, в т.ч. персональных данных организовывается на основании утвержденных директором перечней лиц, имеющих право доступа в указанные помещения. 3.3 На момент присутствия посторонних лиц в помещениях, в которых ведется обработка конфиденциальной информации, в т.ч. персональных данных должны быть приняты меры по недопущению ознакомления посторонних лиц с защищаемой информацией (мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке или накрыты чистыми листами бумаги).

3.4 Вскрытие помещения в начале рабочего дня осуществляется должностным лицом, имеющим право доступа в помещение в соответствии с утвержденными перечнями.

3.5 По окончании рабочего дня все помещения, в которых осуществляется обработка конфиденциальной информации, в т.ч. персональных данных, а также установленные в них хранилища должны быть закрыты на замок и опечатаны.

Помещения, которые оборудованы соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии, ставятся на контроль системы контроля и управлением доступа и опечатыванию не подлежат.

При этом все окна и двери в смежные помещения должны быть надёжно закрыты, съемные носители информации должны быть убраны в запираемые хранилища (сейфы), компьютеры выключены.

3.6 В нерабочее время помещения, в которых осуществляется обработка и хранение конфиденциальной информации, в т.ч. персональных данных вскрываются сотрудниками МКОУ «СОШ №21» в соответствии с перечнями лиц, имеющими право доступа в помещения.

В случае отсутствия вышеуказанного должностного лиц помещение вскрывается комиссионно в составе двух сотрудников школы, один из которых директор или должностное лицо категории заместитель директора. По окончании выполнения работ помещение закрывается комиссионно в соответствии с требованиями пункта 3.5 настоящего Порядка и в первый рабочий день доводятся причины вскрытия помещения до сотрудника , в ведении которого находится вскрывавшееся помещение.

3.7 Для защиты помещений, в которых расположены СВТ, задействованные для обработки конфиденциальной информации, в т.ч. персональных данных, должны приниматься меры для минимизации воздействий огня, дыма, воды, пыли, взрыва, химических веществ, а также кражи.

3.8 В случае прибытия на работу и выявления нарушений целостности дверного полотна (замка) или деформацию технических устройств контроля в помещении, в

котором обрабатывается конфиденциальная информация, в т.ч. персональные данные, необходимо произвести осмотр помещения в присутствии должностного лица, отвечающего за охрану здания, проанализировать степень причинённого ущерба и немедленно уведомить о произошедшем директора МКОУ «СОШ №21».

Должностные лица МКОУ «СОШ №21» должны оценить возможность компрометации хранящихся ключевых и других документов, составить акт, принять при необходимости меры к локализации последствий компрометации конфиденциальной информации и к замене скомпрометированных криптоключей.

3.9. СВТ, предназначенные для обработки конфиденциальной информации с использованием СКЗИ, и размещенное совместно с ними вспомогательное оборудование должны подвергаться регулярным осмотрам с целью выявлений изменения их конфигурации (замки на коммутационных шкафах, использование специальных защитных знаков, пломбирование, опечатывание и др.). В случае обнаружения не соответствий в конфигурации технических средств необходимо прекратить обработку конфиденциальной информации и проинформировать директора школы.

3.10. Должностные лица МКОУ «СОШ №21», имеющие право доступа в помещения, в которых ведется обработка защищаемой информации, не должны оставлять в нем без присмотра посторонних лиц, не уполномоченных на обработку конфиденциальной информации, в т. ч. персональных данных.

3.11. Доступ посторонних лиц в помещения, в которых обрабатывается защищаемая информация, а также используются СКЗИ, должен осуществляться только по служебной необходимости в присутствии сотрудника, имеющего право доступа в данное помещение на основании утвержденных директором школы перечней.

3.12. В случае возникновения нештатной ситуации необходимо незамедлительно сообщать о случившемся дежурному администратору, а также директору МКОУ «СОШ №21».

Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» при угрозе жизни и здоровью сотрудников МКОУ «СОШ №21» допускаются в помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи.

3.13 При утрате ключа от хранилища или от входной двери помещения, в которых обрабатывается конфиденциальная информация, в т.ч. персональные данные, замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей, с документальным оформлением.

Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает директор школы.

Приложение 4
к приказу от 23. 08.2024 № 01-10-215

Должностная инструкция ответственного за организацию обработки персональных данных

1. Общие положения

1.1. Должностная инструкция ответственного за организацию обработки персональных данных (далее – Инструкция) в МКОУ «СОШ №21» определяет ответственность, права и обязанности ответственного за организацию обработки персональных данных в МКОУ «СОШ №21».

1.2. Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении 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».

1.3. Ответственный за организацию обработки персональных данных (далее – Ответственный) относится к категории административно-управленческого аппарата и непосредственно подчиняется директору МКОУ «СОШ №21».

1.4. Ответственный назначается на должность из числа штатных сотрудников приказом директора МКОУ «СОШ №21».

1.5. На время отсутствия Ответственного его обязанности исполняет лицо, назначенное в установленном порядке приказом директорашколы, которое приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

1.6. Ответственный в своей работе руководствуется:

- ❖ федеральными и региональными нормативными, правовыми актами, регулирующими вопросы в области обеспечения безопасности персональных данных;
- ❖ методическими материалами по вопросам защиты информации;
- ❖ приказами и распоряжениями директораМКОУ «СОШ №21»;
- ❖ настоящей Инструкцией.

2. Должностные обязанности

Ответственный должен:

2.1. Знать и соблюдать требования действующего законодательства Российской Федерации в области персональных данных и защиты информации, порядок систематизации, учета и ведения документации, в том числе с использованием современных информационных технологий, правила и нормы охраны труда.

2.2. Осуществлять контроль соблюдения в МКОУ «СОШ №21» законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных и правил их обработки.

2.3. Проводить периодические проверки соответствия обработки персональных данных установленным требованиям в МКОУ «СОШ №21». 2.4. Доводить до сведения, разъяснять работникам МКОУ «СОШ №21» положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

2.5. Проводить инструктажи и занятия по изучению правовой базы по защите персональных данных с сотрудниками МКОУ «СОШ №21», имеющими доступ к персональным данным, и вести Журнал проведения инструктажей по информационной безопасности.

2.6. Участвовать в проведении расследований случаев несанкционированного доступа к персональным данным и других нарушений правил обработки персональных данных.

2.7. Не допускать к работе с персональными данными лиц, не обладающих для этого соответствующими правами.

2.8. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.9. Осуществлять методическое руководство работой администраторов безопасности и администраторов информационных систем персональных данных МКОУ «СОШ №21» в области защиты персональных данных.

3. Права работника Ответственный имеет право:

3.1. Требовать от сотрудников МКОУ «СОШ №21» соблюдения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, правил их обработки и других нормативных документов в области обработки и защиты персональных данных.

3.2. Знакомиться с проектами решений директора МКОУ «СОШ №21», касающимися его деятельности.

3.3. Вносить на рассмотрение директора МКОУ «СОШ №21» предложения по совершенствованию работы, связанной с обязанностями, предусмотренными настоящей Инструкцией.

3.4. Подписывать и визировать документы в пределах своей компетенции. 3.5. Осуществлять взаимодействие с руководителями всех структурных подразделений МКОУ «СОШ №21», получать информацию и документы, необходимые для выполнения своих должностных обязанностей.

3.6. Требовать от директора МКОУ «СОШ №21» оказания содействия в исполнении своих должностных обязанностей и прав.

3.7. Повышать свою профессиональную квалификацию.

3.8. Требовать организованное рабочее место, соответствующее нормам охраны труда.

3.9. Требовать соответствия нормам Трудового Законодательства.

4. Ответственность работника

Работник несет ответственность:

4.1. За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, в пределах, определенных трудовым законодательством Российской Федерации.

4.2. За причинение материального ущерба работодателю, в пределах, определенных действующим трудовым, уголовным и гражданским законодательством Российской Федерации.

4.3. За совершенные в процессе осуществления своей деятельности правонарушения в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

Приложение 5
к приказу от 23. 08.2024 № 01-10-215

Инструкция по организации антивирусной защиты

1. Общие положения

1.1 Настоящая Инструкция устанавливает требования к организации антивирусной защиты и требования к порядку проведения антивирусного контроля в МКОУ «СОШ №21».

2. Порядок организации антивирусной защиты

2.1 Для организации антивирусной защиты в МКОУ «СОШ №21» допускаются к использованию только лицензионное программное обеспечение.

2.2 Антивирусное средство защиты должно быть установлено на все средства вычислительной техники (далее – СВТ), используемые для обработки персональных данных в МКОУ «СОШ №21».

2.3 Установку, а также администрирование средств антивирусной защиты осуществляет инженер-электроник, назначенный приказом директора школы (далее – администратор безопасности).

2.4. Администратор безопасности МКОУ «СОШ №21» должен регулярно осуществлять или организовывать периодическое обновление антивирусных баз и контроль их работоспособностью, а также проводить периодическое тестирование всего установленного программного обеспечения и дискового пространства на предмет отсутствия компьютерных вирусов.

3. Порядок проведения антивирусного контроля

3.1. Ежедневно в начале работы при загрузке компьютера (для серверов локально-вычислительной сети – при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.

3.2. Антивирусный контроль входящей и исходящей информации должен проводиться непосредственно после получения информации и перед отправкой (записью на съемный носитель) путем нажатия правой клавишей мыши на нужный файл (папку) и выбора из контекстного меню пункта «Проверить на вирусы».

3.3. При работе со съемными носителями информации пользователь обязан перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов и иных вредоносных программ путем автоматической проверки флеш-носителей с помощью программного средства USB Disk Security или путем выбора из всплывающего окна пункта «Проверить и исправить ошибки» при подключении устройства к СВТ.

3.4. Еженедельно администратор безопасности организовывает проведение плановой полной проверки СВТ, а также всех подключаемых носителей информации к данному СВТ на наличие или отсутствие вирусов.

3.5. При возникновении подозрения на наличие в системе компьютерного вируса (нетипичная работа программ, искажение данных, частое появление сообщений о системных ошибках и т.п.) пользователем должен быть проведён внеплановый антивирусный контроль СВТ. При необходимости для определения факта наличия или отсутствия вируса может быть привлечен администратор безопасности.

3.6. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- ❖ приостановить работу;

- ❖ поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также смежные отделы, использующие эти файлы в работе.

3.7. При обнаружении зараженных файлов администратор безопасности обязан:

- ❖ отключить Интернет соединение, в том числе подключение по локальной сети;
- ❖ поместить зараженные файлы в карантин;
- ❖ провести «лечение» или уничтожение зараженных файлов, а затем осуществить повторную проверку;
- ❖ в случае обнаружения на СВТ или на съемном носителе информации вируса, не поддающегося «лечению», в возможно короткие сроки обновить пакет антивирусных программ и провести повторное «лечение» зараженных файлов;
- ❖ при необходимости выполнить восстановление системы или переустановку операционной системы;
- ❖ по факту обнаружения зараженных вирусом файлов составить служебную записку на имя директора МКОУ «СОШ №21», в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3.8. Пользователю СВТ запрещается:

- ❖ изменять настройки и конфигурацию средств антивирусной защиты;
- ❖ удалять или добавлять в систему какие-либо другие средства антивирусной защиты;
- ❖ использовать на СВТ съемные носители информации без предварительной проверки;
- ❖ запускать неизвестные файлы, пришедшие по электронной почте;
- ❖ игнорировать проведение антивирусных проверок СВТ, а также всплывающие уведомления средства антивирусного контроля.

4. Ответственность

4.1 Администратор безопасности, а также пользователи несут ответственность за проведение мероприятий по антивирусному контролю, а также за ненадлежащее исполнение или неисполнение обязанностей, предусмотренных настоящей Инструкцией в рамках ст. 192 Трудового Кодекса Российской Федерации и ст. 273, 274 Уголовного кодекса Российской Федерации.

Приложение 6 к приказу
к приказу от 23. 08.2024 № 01-10-215

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Общие положения

1.1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МКОУ «СОШ №21» (далее – Правила) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.2. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в МКОУ «СОШ №21» осуществляется проведение периодических проверок условий обработки персональных данных.

2.2. Проверки осуществляются ответственным за организацию обработки персональных данных в МКОУ «СОШ №21» либо комиссией, образуемой приказом директора МКОУ «СОШ №21». В проведении проверки не может участвовать сотрудники, прямо или косвенно заинтересованные в её результатах.

2.3. Проверки соответствия обработки персональных данных установленным требованиям в МКОУ «СОШ №21» проводятся на основании утвержденного директором ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям (плановые проверки) или на основании поступившего в МКОУ «СОШ №21» письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

2.4. Проведение плановой проверки осуществляется не реже одного раза в год.

2.5. Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

2.6. Проверки условий обработки персональных данных осуществляются непосредственно на месте обработки персональных данных путем опроса либо при необходимости путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

2.7. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть 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 до ввода в эксплуатацию информационной системы 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.

2.8. Ответственный за организацию обработки персональных данных в МКОУ «СОШ №21» (комиссия) имеет право:

запрашивать у сотрудников информацию, необходимую для реализации полномочий;

требовать от уполномоченных за обработку персональных данных должностных лиц 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;

вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

2.9. Срок проведения проверки не может составлять более 30 дней со дня принятия решения о её проведении.

2.10. По результатам каждой проверки составляется протокол проведения внутренней проверки.

2.11. При выявлении в ходе проверки нарушений в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

2.12. Председатель комиссии по организации работы, связанной с обработкой персональных данных, либо работник, ответственный за организацию работы с персональными данными, проводившие проверку, информируют директора о результатах проверки и мерах, необходимых для устранения нарушений, и представляет на утверждение протокол проведения внутренней проверки. 2.13. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в МКОУ «СОШ №21» (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

С приказом **МКОУ «СОШ № 21»** от 26.08.2025 г. **№ 01-10-279**

ознакомлены:

ФИО Сундукова Р.И. подпись

ФИО Гутаева А.М. подпись

ФИО Мажиева А.А. подпись

ФИО Казанчева М.Х. подпись

ФИО Бегидова Л.С. подпись

ФИО Шаова Ф.В подпись

ФИО Гериева А.И подпись

ФИО Альборова И.Б подпись

ФИО Батырова А.В подпись

ФИО Махмудова Ю.Р. подпись

ФИО Блиаева З.А подпись

ФИО Башиева О.А подпись

ФИО Варосян М.Т. подпись

ФИО Пшорцева В.В. подпись

ФИО Кушхова О.Н. подпись

ФИО Мударисова М.М. подпись

ФИО Хамукова Ф.Л. подпись

ФИО Бурнакова Т.Б. подпись

ФИО Жабоева Л.Ч. подпись

ФИО Хатохова Р.А подпись

ФИО Канцежева А.М. подпись

ФИО Хазова А.С. подпись

ФИО Жанчева З.А. подпись

ФИО Машхолова Ф.Р подпись

ФИО Мартокова М.Х. подпись

струнаев Г.В

Жанчукова К.К.