КГБОУ «Новоалтайская общеобразовательная школа-интернат»

ПРИКАЗ

03.03.2023 № 35

Новоалтайск

«О создании комиссии по защите персональных данных и назначении ответственных за обработку персональных данных работников, обучающихся, воспитанников и их родителей (законных представителей) в КГБОУ «Новоалтайская общеобразовательная школа-интернат»

С целью организации обработки персональных данных в КГБОУ «Новоалтайская общеобразовательная школа-интернат» в соответствии с пунктом 1 части 1 статьи 18.1 и части 1 статьи 22.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», постановления Правительства РФ от 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ

1. Создать комиссию по защите персональных данных работников школы-интерната и всех участников образовательного процесса с наделением ее полномочиями по проведению мероприятий, касающихся организации защиты персональных данных в составе:

Председатель:

Некрасова О.Н., директор школы-интерната.

Члены комиссии:

Соболева И.Е., главный бухгалтер;

Киснер О.Г., заместитель директора по УВР;

Хаблак И.С., инспектор по кадрам.

1.1. Утвердить план внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение №1).

2. Возложить персональную ответственность за защиту персональных данных и допустить к обработке персональных данных сотрудников следующих сотрудников школы-интерната (Приложение №2):

2.1. Лица, ответственные за защиту информационных систем:

Савко В.М., педагог-психолог, администратор школьного сайта (Приложения №3, №4).

2.2. Лица, ответственные за защиту персональных данных по сотрудникам и обучающимся, воспитанникам школы-интерната:

2.2.1. Некрасова О.Н., директор школы-интерната, Киснер О.Г., заместитель директора по УВР: тарификационные данные, сведения для расчета заработной платы; все персональные данные по сотрудникам, данные о преподаваемых предметах, о дополнительной педагогической нагрузке, научно-методической работе, сведения об образовании, стаже, аттестации и повышении квалификации, данные о наградах и достижениях, все персональные данные по обучающимся, все данные на молодых специалистов и вновь прибывших учителей;

2.2.2. Соболева И.Е., главный бухгалтер: тарификационные данные, сведения для расчета заработной платы, данные налогоплательщика, данные в ПФР;

2.2.3. Ветров А.И., заместитель директора по АХР: персональные данные на сотрудников;

2.2.4. Хаблак И.С., инспектор по кадрам: все персональные данные на сотрудников, обучающихся, воспитанников, родителей (законных представителей);

2.2.5. Чичерина Е.Ф., социальный педагог: данные о социальных и жилищных условиях, о материальном положении обучающихся, воспитанников; все персональные данные по обучающимся, воспитанникам и их родителей (законных представителей);

2.2.6. Педагоги-психологи: персональные данные на обучающихся и их родителей (законных представителей);

2.2.7. Классные руководители, воспитатели: все персональные данные на обучающихся и их родителей (законных представителей) своих классов;

2.2.8. Медицинские работники: персональные медицинские данные обучающихся, воспитанников школы-интерната;

2.2.9. Вахтеры: персональные данные на обучающихся и их родителей (законных представителей), сотрудников и посетителей.

3. Материалы, содержащие персональные данные сотрудников или обучающихся для школьного сайта, размещаются с письменного согласия сотрудников, обучающихся, воспитанников и их родителей (законных представителей).

4. Инспектору по кадрам Хаблак И.С. внести в должностные инструкции ответственных за обработку персональных данных изменения в соответствии с п.2 настоящего приказа.

5. Утвердить Акт оценки вреда субъектам персональных данных (приложение №5).

6. Инспектору по кадрам Хаблак И.С. ознакомить всех заинтересованных лиц с настоящим приказом.

7. Контроль за исполнением приказа оставляю за собой.

Директор школы-интерната

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 13D9CC154DA9D2D851D320551713786D
Владелец: Некрасова Ольга Николаевна
Действителен: с 14.02.2023 до 09.05.2024

Некрасова О.Н.

Приложение 1 к приказу
№ 35 от 03.03.2023

ПЛАН
внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

Мероприятие	Периодичность плановых мероприятий	Исполнитель
Контроль соблюдения правил доступа к ПДн	2 раза в год (сентябрь, март)	Ответственные за обеспечение безопасности персональных данных обучающихся, воспитанников и работников Киснер О.Г., Хаблак И.С.
Контроль соблюдения режима защиты	2 раза в год (сентябрь, март)	Ответственный за обеспечение безопасности персональных данных информационных систем Савко В.М.
Контроль выполнения антивирусной политики	2 раза в год (сентябрь, март)	Ответственный за обеспечение безопасности персональных данных информационных систем Савко В.М.
Контроль обновления ПО и единообразия применяемого ПО	2 раза в год (сентябрь, март)	Ответственный за обеспечение безопасности персональных данных информационных систем Савко В.М.
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	Ответственный за обеспечение безопасности персональных данных информационных систем Савко В.М.
Поддержание в актуальном состоянии нормативно-организационных документов	Ежегодно	Заместитель директора по УВР Киснер О.Г. Инспектор по кадрам Хаблак И.С.

ПРОТОКОЛ № ____
проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных
в КГБОУ ««Новоалтайская общеобразовательная школа-интернат»

Настоящий Протокол составлен в том, что «__» _____20___г.
Комиссией в составе: _____
_____
_____
(должность, Ф.И.О. сотрудников)
проведена проверка _____
_____
(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 О.Н. Некрасова

Члены комиссии:
Соболева И.Е., главный бухгалтер, заместитель председателя _____
Члены комиссии:
Киснер О.Г., заместитель директора по УВР _____
Хаблак И.С., инспектор по кадрам_____

Приложение 2 к приказу
№ 35 от 03.03.2023

Список должностных лиц, допущенных к обработке персональных данных
в КГБОУ «Новоалтайская общеобразовательная школа-интернат»

Должность	Ф.И.О.	Группа обрабатываемых данных
Директор	Некрасова О.Н.	Все персональные данные
Заместитель директора по УВР	Киснер О.Г.	Все персональные данные
Главный бухгалтер Бухгалтер	Соболева И.Е. Кириченко Е.А.	Персональные данные работников
Заместитель директора по АХР	Ветров А.И.	Персональные данные на сотрудников
Инспектор по кадрам	Хаблак И.С.	Все персональные данные
Социальный педагог	Чичерина Е.Ф.	Персональные данные обучающихся, воспитанников и их родителей (законных представителей)
Педагоги-психологи	Савко В.М. Стадник Т.О.	Персональные данные обучающихся, воспитанников и их родителей (законных представителей)
Медработники	Кравцова И.И. Краюшкина Л.В. Макарова Г.И.	Персональные данные обучающихся, воспитанников и их родителей (законных представителей)
Вахтеры	Орлова З.В. Кормакова Т.С.	Персональные данные на обучающихся и их родителей (законных представителей), сотрудников и посетителей.
Классные руководители	Агафонова С.М.	Персональные данные обучающихся, воспитанников и их родителей (законных представителей)
	Васильева О.И.	
	Илинчук С.А.	
	Нестерова В.В.	
	Пупарева А.И.	
	Рахматуллоева О.П.	
	Сазанюк В.Д.	
	Стадниченко Н.П.	
	Хилюкова Н.Л.	
Воспитатели	Аладышкина Н.В.	
	Вист И.В.	
	Жиглова М.В.	
	Згода С.А.	
	Петрачук Т.В.	
	Свиридова Л.Л.	
	Сергиенко А.А.	
	Токарева Т.М.	
	Тюкавкина М.И.	
	Чернова Н.В.	
	Шефер Г.М.	
	Шолохова О.А.	

Педагоги дополнительного образования	Прохорова Н.Н. Снегирева А.Е.	
Педагоги	Адова И.А.	
	Матовникова Е.В.	
	Сим В.П.	
	Ситникова А.А.	
	Тронина О.И.	

Приложение 3 к приказу
№ 35 от 03.03.2023

Инструкция
администратора безопасности информационных систем персональных данных КГБОУ «Новоалтайская общеобразовательная школа-интернат»

I. ОБЩИЕ ПОЛОЖЕНИЯ

Данная Инструкция определяет основные обязанности и права администратора безопасности информационных систем персональных данных КГБОУ «Новоалтайская общеобразовательная школа-интернат» (далее – школа-интернат)

1.1. Администратор безопасности информационных систем персональных данных (далее – ИСПДн) назначается приказом директора школы-интерната.

1.2. Решение вопросов обеспечения информационной безопасности входит в служебные обязанности администратора безопасности ИСПДн.

1.3. Администратор безопасности ИСПДн обладает правами доступа к любым программным и аппаратным ресурсам школы-интерната.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.2. **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) *(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

2.3. **Доступ к информации** – возможность получения информации и её использования *(ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).*

2.4. **Защита информации** — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.5. **Информация** - сведения (сообщения, данные) независимо от формы их представления *(ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).*

2.6. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств *(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

2.7. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

2.8. **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.

2.9. **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

2.10. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

2.11. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.12. **Угрозы безопасности персональных данных (УБПДн)** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных (*Методика определения актуальных угроз безопасности персональных дан-*

ных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.))

2.13. **Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

III. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Администратор безопасности ИСПДн обязан:

3.1. Знать перечень и условия обработки персональных данных в Школе-интернате.

3.2. Знать перечень установленных в кабинетах школы-интерната технических средств, в том числе съёмных носителей, конфигурацию ИСПДн и перечень задач, решаемых с её использованием.

3.3. Определять полномочия пользователей ИСПДн (оформление разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей.

3.4. Осуществлять учёт и периодический контроль над составом и полномочиями пользователей автоматизированных рабочих мест (далее АРМ).

3.5. Осуществлять оперативный контроль за работой пользователей, защищённых АРМ и адекватно реагировать на возникающие нештатные ситуации.

3.6. Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

3.7. Реагировать на попытки несанкционированного доступа к информации в установленном ст. 4 настоящей Инструкции.

3.8. Устанавливать и осуществлять настройку средств защиты информации в рамках компетенции.

3.9. Осуществлять непосредственное управление и контроль режимов работы функционирования применяемых в ИСПДн средств защиты информации, осуществлять проверку правильности их настройки (выборочное тестирование).

3.10. Периодически контролировать целостность печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных.

3.11. Проводить работу по выявлению возможных каналов утечки персональных данных, изучать текущие тенденции в области защиты персональных данных.

3.12. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

3.13. Предоставлять доступ к ИСПДн новым пользователям, предоставлять им возможность задать пароль, соответствующий требованиям «Инструкции по организации парольной защиты».

3.14. Производить мероприятия по внеплановой смене паролей в соответствии с «Инструкцией по организации парольной защиты».

3.15. Вносить плановые и внеплановые изменения в учётную запись пользователей ИСПДн, в том числе по требованию руководителя отдела и в случае увольнения сотрудника.

3.16. Осуществлять периодическое резервное копирование баз персональных данных и сопутствующей защищаемой информации, а также осуществлять внеплановое создание резервных копий по требованию пользователей ИСПДн и в иных случаях, когда это необходимо для обеспечения сохранности персональных данных.

3.17. Осуществлять восстановление информации из резервных копий по требованию пользователей ИСПДн и в иных случаях, когда это необходимо для восстановления утраченных сведений.

3.18. Хранить дистрибутивы программного обеспечения, установленного в ИСПДн, в том числе дистрибутивы средств защиты информации, в месте, исключающем несанкционированный доступ к ним третьих лиц.

3.19. Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.

3.20. Знать законодательство РФ о персональных данных, следить за его изменениями.

3.21. Выполнять иные мероприятия, требуемые техническими и программными средствами ИСПДн для поддержания их функционирования.

IV. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. Сеансы работы с Исподн незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

4.1.2. Действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа администратор безопасности ИСПДн обязан:

4.2.1. Прекратить несанкционированный доступ к ИСПДн;

4.2.2. доложить директору Школы-интерната о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях.

V. ПРАВА

Администратор безопасности ИСПДн имеет право:

5.1. Требовать от пользователей ИСПДн выполнения инструкций в части работы с программными, аппаратными средствами ИСПДн и персональными данными.

5.2. Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.

5.3. Проводить внеплановые антивирусные проверки при возникновении угрозы появления вредоносных программ.

5.4. Производить периодические попытки взлома паролей пользователей в целях тестирования системы контроля доступа на наличие уязвимостей. В случае успешной попытки – вправе требовать у пользователя изменения пароля.

5.5. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

VI. ОТВЕТСТВЕННОСТЬ

6.1. Администратор безопасности ИСПДн несёт персональную ответственность за соблюдение требований настоящей Инструкции, за средства защиты информации, применяемые в Школе-интернате, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

6.2. Администратор безопасности ИСПДн при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Ознакомлен _____ _____

Ф.И.О. подпись

Приложение 4 к приказу
№ 35 от 03.03.2023

Инструкция
по парольной защите информации в автоматизированных системах
КГБОУ «Новоалтайская общеобразовательная школа-интернат»

Обозначения и сокращения

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

АС – автоматизированная система

АСО – активное сетевое оборудование

АСУ – автоматизированная система управления

БД – база данных

ВТСС – вспомогательные технические средства и системы

ЗИ – защита информации

ИБ – информационная безопасность

ИБП – источник бесперебойного питания

Инструкция – Инструкция по парольной защите информации в автоматизированных системах КГБОУ «Новоалтайская общеобразовательная школа-интернат»

КЗ – контролируемая зона

КСЗИ – комплекс средств защиты информации

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

Директор – директор КГБОУ «Новоалтайская общеобразовательная школа-интернат»

ОИ - объект информатизации

ПАК – программно-аппаратный комплекс

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

Устав – Устав КГБОУ «Новоалтайская общеобразовательная школа-интернат»

ППО – прикладное программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

ПЭВМ – персональная электронно-вычислительная машина

РД – руководящий документ

САЗ – система анализа защищенности

СВТ – средства вычислительной техники

СЗИ – средства защиты информации

СОВ – система обнаружения вторжений

СПО – специальное программное обеспечение

ТКУИ – технические каналы утечки информации

ТС – технические средства АС

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии со Специальными требованиями и рекомендациями по технической защите конфиденциальной информации, утвержденными приказом Председателя Гостехкомиссии России от 30.08.2002 № 282-дсп, Приказа ФСТЭК России от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных», Положения о порядке организации и проведения работ в КГБОУ «Новоалтайская общеобразовательная школа-интернат» по защите информации ограниченного доступа (защищаемой информации) и других нормативных правовых актов и руководящих документов в области защиты информации.

1.2. Инструкция устанавливает требования и ответственность при организации парольной защиты информации, а также определяет порядок контроля за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.3. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности информации, и не исключает обязательного выполнения их требований.

1.4. Требования настоящей Инструкции являются обязательными для исполнения всеми работникам КГБОУ «Новоалтайская общеобразовательная школа-интернат», использующими в своей работе средства вычислительной техники.

1.5. Все работники КГБОУ «Новоалтайская общеобразовательная школа-интернат», использующие в своей работе средства вычислительной техники, должны быть ознакомлены с требования настоящей Инструкции под роспись.

1.6. На основании настоящей Инструкции в подведомственных КГБОУ «Новоалтайская общеобразовательная школа-интернат» учреждениях разрабатывается собственная инструкция об парольной защите информации с учетом специфики построения автоматизированных систем (АС).

1.7. При существенных изменениях, используемых в КГБОУ «Новоалтайская общеобразовательная школа-интернат» информационных технологий, настоящая Инструкция может быть изменена и дополнена.

2. Требования, предъявляемые к идентификаторам (кодам) и паролям (порядок формирования и обращения с ними)

2.1. Авторизация пользователей осуществляется путем ввода идентификатора и пароля.

2.2. При авторизации в АС, предназначенных для обработки информации ограниченного доступа, обязательным дополнительным условием является применение средств усиленной идентификации и аутентификации.

2.3. Требования к формированию паролей и обращению с ними.

2.3.1. В рамках парольной защиты в КГБОУ «Новоалтайская общеобразовательная школа-интернат» пароли бывают первичными и постоянными. Первичный пароль формируется ответственным за безопасность информации и учитывается в журнале учета паролей (Приложение 1) и выдается пользователю в виде карточки паролей (Приложение 2).

2.3.2. Журнал учета паролей разрешается вести в электронном виде. Информация из журнала подлежит защите от несанкционированного доступа.

2.3.3. При создании нового пользователя в обязательном порядке необходимо включить опцию смены пароля при следующем входе пользователя в систему. При следующем входе в систему пользователь формирует постоянный пароль с учетом требований настоящей Инструкции.

2.3.4. В случае отсутствия технической возможности включения данной опции пароль генерируется пользователем самостоятельно с учетом требований настоящей Инструкции.

2.3.5. Постоянный пароль является личным паролем. Владельцы личных паролей обязаны обеспечивать их тайну.

2.3.6. Первичные и постоянные пароли в КГБОУ «Новоалтайская общеобразовательная школа-интернат» генерируются с учетом следующих требований:

- пароль должен знать только его владелец (при самостоятельном выборе пароля пользователем);
- пароль работник вводит собственноручно (при самостоятельном выборе пароля пользователем);
- длина пароля должна быть не менее 6 символов;
- должна быть соблюдена сложность пароля (в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры);
- пароль не должен включать смысловую нагрузку (имена, фамилии, наименования организаций, улиц, городов и т.д.), общепринятые сокращения (user01, password02 и т.п.) и последовательные сочетания клавиш клавиатуры (qwerty01, Йцукен12);
- пароль невозможно использовать повторно до тех пор, пока не будет создано 4 других пароля;
- количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя должно быть не более 10;
- пользователь не имеет права сообщать свой личный пароль никому.

2.3.7. Требования к формированию паролей обеспечиваются техническими возможностями используемых операционных систем, средств защиты информации и информационных ресурсов (например, 1С-Предприятие, СУФД Федерального казначейства и т.п.).

2.3.8. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в три месяца. Внеплановая смена пароля производится по требованию ответственного за парольную защиту, в случае его компрометации, а также по просьбе пользователя. Для внеплановой смены пароля по просьбе пользователь должен представить ответственному за безопасность информации служебную записку с указанием причины замены пароля.

2.3.9. Хранение работниками КГБОУ «Новоалтайская общеобразовательная школа-интернат» значений своих паролей на бумажном носителе ЗАПРЕЩЕНО.

2.3.10. Администраторские пароли (пароли системных администраторов, администраторов баз данных (информационных ресурсов), администраторов безопасности) должны храниться на бумажных носителях в опечатанных конвертах из плотной бумаги. При этом хранение должно быть только в личном, опечатанном владельцем пароля сейфе или надежно запираемом металлическом шкафу либо в пенале, опечатанном личной печатью (возможно вместе с персональными идентификаторами).

2.3.11. Разрешается хранение администраторских паролей у непосредственного руководителя владельца администраторского пароля при соблюдении вышеперечисленных требований.

2.3.12. Требования к порядку формирования и обращения с паролями и идентификаторами распространяются как на порядок работы в АС, так и на порядок работы с информационными ресурсами (например, 1С-Предприятие, СУФД Федерального казначейства и т.п.), требующих процедуры авторизации.

2.3.13. При авторизации при работе с информационным ресурсом генерация паролей осуществляется администратором этих баз данных и ресурсов. Требования настоящей Инструкции при формировании паролей должны быть учтены при администрирова-

нии информационных ресурсов сторонней организацией (аутсорсинг). Администраторские пароли должны храниться согласно требованиям настоящей Инструкции у ответственного за безопасность информации.

2.4. Требования к идентификаторам и обращению с ними.

2.4.1. В КГБОУ «Новоалтайская общеобразовательная школа-интернат» для идентификации применяются логин (имя пользователя) и средства усиленной идентификации и аутентификации (программные, программно-аппаратные), в том числе электронные персональные идентификаторы (типа _____, и т.п.).

2.4.2. При использовании средств усиленной идентификации и аутентификации в АС, предназначенных для обработки информации ограниченного доступа, программное обеспечение идентификации и аутентификации и электронные персональные идентификаторы должны быть сертифицированы в системе сертификации ФСТЭК России.

2.4.3. Структура идентификаторов определяется возможностями и требованиями программного и (или) программно-аппаратного обеспечения электронных персональных идентификаторов и средств аутентификации применяемых операционных систем и приложений.

2.4.4. При использовании для генерации паролей программного и (или) программно-аппаратного обеспечения электронных персональных идентификаторов структура паролей определяется его возможностями.

2.4.5. При использовании электронные персональные идентификаторы для хранения паролей обязательно выполнение требований к первичным и постоянным паролям.

2.4.6. PIN-код электронного персонального идентификатора устанавливается (изменяется) его пользователем. Пользователь обязан сохранять действующий PIN - код используемого электронного персонального идентификатора в тайне.

2.4.7. PIN-код электронного персонального идентификатора должен соответствовать требованиям стойкости, рекомендованным эксплуатационной документацией на устройство.

2.4.8. Электронные персональные идентификаторы учитываются и выдаются работникам КГБОУ «Новоалтайская общеобразовательная школа-интернат» по журналу учета (Приложение 3).

2.4.9. Пользователи электронных персональных идентификаторов обязаны обеспечивать их сохранность и исключать возможность неконтролируемого их использования.

2.5. Порядок смены паролей и идентификаторов при изменениях в организационно-штатной структуре КГБОУ «Новоалтайская общеобразовательная школа-интернат» (кадровые перестановки, увольнение).

2.5.1. При прекращении трудового договора с работником КГБОУ «Новоалтайская общеобразовательная школа-интернат» все созданные для этого работника учетные записи (пользовательское имя) во всех АС и информационных ресурсах подлежат блокированию не позднее, чем в день увольнения работника. Полное удаление учетных записей производится в течении 5 рабочих дней со дня увольнения работника. Основанием для блокирования и последующего удаления учетных записей служащего является заявка, представленная непосредственным руководителем увольняемого работника не позднее, чем за 3 рабочих дня до дня его увольнения.

2.5.2. При проведении организационно-штатных мероприятий (кадровые перестановки) непосредственный руководитель структурного подразделения обязан представить ответственному за безопасность информации заявку на изменение в правах доступа.

2.5.3. Формы заявок, сроки и порядок их отработки определяются установленными в КГБОУ «Новоалтайская общеобразовательная школа-интернат» правилами разрешительной системе допуска пользователей (обслуживающего персонала) к информационным ресурсам и автоматизированным системам, а также должностным инструкциям ответственным исполнителям.

2.6. Порядок действий при компрометации идентификаторов и паролей.

2.6.1. Под компрометацией понимается: утрата пароля и (или) идентификатора, разглашение пароля или PIN-кода идентификатора (явная компрометация), или иная си-

туация, которая дает основание для предположения о нарушении конфиденциальности паролей, идентификаторов или PIN-кода идентификатора (неявная компрометация).

2.6.2. При выявлении факта утраты пароля, разглашения пароля, PIN-кода идентификатора, самого идентификатора работники КГБОУ «Новоалтайская общеобразовательная школа-интернат» обязаны незамедлительно сообщить о данных фактах своему непосредственному руководителю и ответственному за парольную защиту.

2.6.3. В случае выявления факта компрометации идентификаторов и паролей пользователя ответственный за безопасность информации обязан немедленно заблокировать учетную запись данного пользователя.

2.6.4. При подозрении на компрометацию пользовательского пароля незамедлительно производится внеплановая смена пароля для этого пользователя.

2.6.5. При подозрении на компрометацию любого из администраторских паролей и идентификаторов и в случае выявления факта компрометации администраторских идентификаторов и паролей незамедлительно производится внеплановая смена всех администраторских паролей.

2.6.6. При явной компрометации проводится служебное расследование.

2.6.7. Расследование факта компрометации проводится комиссией, назначаемой приказом директора. В состав комиссии в обязательном порядке включается ответственный за безопасность информации, работник, обнаруживший факт компрометации, непосредственный руководитель работника, допустившего факт компрометации и заместитель директора. При необходимости в состав комиссии могут включаться другие работники КГБОУ «Новоалтайская общеобразовательная школа-интернат».

2.6.8. Результаты работы комиссии оформляются актом. Акт подлежит утверждению директором.

2.6.9. В процессе работы комиссии обязательными для установления являются:

- дата и время компрометации;
- ФИО, должность и подразделение работника, допустившего факт компрометации;
- уровень критичности компрометации;
- обстоятельства, способствовавшие совершению компрометации;
- информационные ресурсы, затронутые компрометацией;
- характер и размер реального и потенциального ущерба.

2.6.10. В течение 5 (пяти) рабочих дней с момента назначения начала работы комиссии у работника, допустившего факт компрометации пароля, запрашивается объяснительная записка (путем письменного запроса на имя непосредственного руководителя данного работника). Объяснительная записка должна быть представлена комиссии в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа предоставить объяснительную записку, данный факт отражается в акте.

2.6.11. Уничтожение актов на уничтожение материалов расследования фактов компрометации осуществляется в соответствии с установленными требованиями по делопроизводству и номенклатурой дел.

3. Права и обязанности ответственного за безопасность информации и пользователей автоматизированных систем

3.1. Основные задачи ответственного за безопасность информации:

- организация установки средств идентификации и аутентификации (если это обусловлено требованиями действующего законодательства и внутренними организационными документами КГБОУ «Новоалтайская общеобразовательная школа-интернат» в области защиты информации);
- организация парольной защиты во всех автоматизированных системах и информационных ресурсах КГБОУ «Новоалтайская общеобразовательная школа-интернат»;
- формирование паролей и PIN-кодов электронных персональных идентификаторов в соответствии с требованиями настоящей Инструкции;

- учет и выдача первичных паролей, и электронных персональных идентификаторов и PIN-кодов к ним;
- осуществление контроля за состоянием системы парольной защиты информации в КГБОУ «Новоалтайская общеобразовательная школа-интернат».

3.2. Ответственный за безопасность информации имеет право:

- вносить предложения по совершенствованию системы парольной защиты информации в КГБОУ «Новоалтайская общеобразовательная школа-интернат»;
- принимать участие в планировании мероприятий по парольной защите информации в КГБОУ «Новоалтайская общеобразовательная школа-интернат» и планировании оснащения средствами идентификации и аутентификации;
- осуществлять контроль состояния средств идентификации и аутентификации в структурных подразделениях КГБОУ «Новоалтайская общеобразовательная школа-интернат»;
- проводить служебные проверки по фактам компрометации;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств идентификации и аутентификации.

3.3. Обязанности в части парольной защиты информации должны быть отражены в должностной инструкции (регламенте) ответственного за безопасность информации.

3.4. Обязанности ответственного за безопасность информации могут быть возложены на следующие должностные лица КГБОУ «Новоалтайская общеобразовательная школа-интернат»:

- администраторы АС;
- администраторы баз данных;
- администраторы безопасности АС.

3.5. Ответственными за безопасность информации в КГБОУ «Новоалтайская общеобразовательная школа-интернат» не могут быть должностные лица сторонних организаций.

3.6. Количество ответственных за безопасность информации не может составлять менее двух человек.

3.7. Работникам КГБОУ «Новоалтайская общеобразовательная школа-интернат» в своей работе запрещается:

- Сообщать кому-либо свой личный пароль и PIN-код к электронному персональному идентификатору;
- передавать кому-либо выданный электронный персональный идентификатор;
- осуществлять вход в операционные системы автоматизированных систем и в информационные ресурсы КГБОУ «Новоалтайская общеобразовательная школа-интернат» под чужими идентификаторами и паролями;
- отключать средства идентификации и аутентификации.

3.8. В случае появления подозрений на факт компрометации пароля, а также в случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств идентификации и аутентификации, работники КГБОУ «Новоалтайская общеобразовательная школа-интернат» обязаны немедленно проинформировать об этом ответственного за безопасность информации.

4. Обязанности и ответственность должностных лиц в рамках системы парольной защиты информации

4.1. Нарушение требований по защите информации (в том числе антивирусной защиты) влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение 1
к Инструкции

Форма журнала учета паролей

№ п/п	ФИО владельца (работника)	Должность	Логин (имя пользователя)	Дата генерации пароля	ФИО, выдавшего пароль	Первичный пароль

Приложение 2
к Инструкции

Форма карточки паролей

Карточка № _____

на период с ___.___.20__г. по ___.___.20__г.

ФИО пользователя

Должность пользователя (полностью)

Идентификатор ресурса	Идентификатор пользователя (Имя Пользователя)	Аутентификатор пользователя (пароль)
(имя информационного ресурса/наименование автоматизированной системы) Образец: АС «Кадровая служба»	Английские буквы	**12Fns*92**

Выдал: ФИО ответственного за парольную защиту _____

«___»_____ 20___ г. (дата генерации пароля) *роспись*

ВНИМАНИЕ!

Указанный пароль является временным, после первичного доступа к ресурсу пароль необходимо сменить на постоянный. ***Пользователь обязан сохранять действующий пароль в тайне****. В случае компрометации пароля (утеря, кража, передача 3-му лицу) пользователь обязан немедленно сообщить об этом ответственному за парольную защиту*
по тел. (_____) _____

Парольную карточку № _____ получил,
с обязательством ознакомлен _____ ФИО пользователя

(дата получения парольной карточки)

Приложение 3
к Инструкции

Форма журнала учета электронных персональных идентификаторов

№ п/п (Уч. №)	Тип идентификатора	Заводской номер	Дата постановки на учет	Дата выдачи	Отметка о получении (ФИО и роспись работника, получающего идентификатор)	Отметка о выдаче (ФИО и роспись работника, ответственного за учет)
1	2	3	4	5	6	7
1.	**eToken**					
2.	**RuToken**					
3.	**iButton**					

Дата приема (возврата)	Отметка о возврате (ФИО и роспись работника, получившего идентификатор)	Отметка о получении (ФИО и роспись работника, ответственного за учет)	Отметка об уничтожении (номер и дата акта об уничтожении идентификатора)	Примечание
8	9	10	11	12

Приложение 5 к приказу
№ 35 от 03.03.2023

Регламент
Резервного копирования персональных данных
КГБОУ «Новоалтайская общеобразовательная школа-интернат»

1. Термины и сокращения

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Типовая информационная система – информационная система, в которой требуется обеспечение только конфиденциальности персональных данных.

Специальная информационная система – информационная система, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

2. Общие положения

Настоящий Регламент определяет порядок резервирования персональных данных (далее – ПДн) в КГБОУ «Новоалтайская общеобразовательная школа-интернат» для последующего восстановления работоспособности информационных систем персональных данных (далее – ИСПДн) при полной или частичной потере информации, определение порядка восстановления персональных данных.

Ответственными за выполнение требований данного Регламента и реализацию указанных в нем процедур являются Администратор безопасности информационных систем персональных данных (далее – Администратор безопасности ИСПДн).

3. Порядок резервного копирования

3.1. Массивы персональных данных, подлежащие резервированию
Резервному копированию подлежит информация, хранящаяся на серверах:
*базы данных;
*каталоги данных на файловых серверах;
*общие каталоги отделов и подразделений.
3.2. Методы и способы создания резервных копий
Резервирование ПДн, хранящихся на серверах, осуществляется путем копирования резервируемой информации на магнитные ленты, RAID-массивы, магнитооптические накопители, съемные диски, дисковые накопители и облачные сервисы.
При резервировании ПДн, хранящихся на серверах, используются две стратегии резервирования:
**горячее резервирование (hotstandby)* – копирование данных основного сервера на резервный сервер при включенных сервисах автоматизированной системы, входящей в состав ИСПДн;
**холодное резервирование (standby backup)* – копирование данных основного сервера на резервный сервер при выключенных сервисах автоматизированной системы, входящей в состав ИСПДн.
Используются следующие методы резервного копирования:
**полное резервирование* – периодически создается полная копия массивов данных;
**добавочное резервирование* – на первом этапе создается полная копия массивов данных, а на последующих этапах в данную копию вносятся изменения в соответствии с произошедшими изменениями.
Также используются следующие способы создания резервных копий:
**ручной* – резервные копии создаются простым копированием массивов данных ответственным работником;
**автоматизированный* – резервные копии создаются ответственным работником с использованием специализированного программного обеспечения;
**автоматический* – резервные копии создаются с использованием специализированного программного обеспечения в соответствии с предварительно настроенным расписанием.
Указанные методы могут использоваться как при создании резервных копий в соответствии с Планом резервного копирования ПДн, так и при создании резервных копий по запросу. Форма Плана приведена в Приложении 1 настоящего Регламента.
3.3. План резервного копирования
В МКОУ Фунтиковская средняя общеобразовательная школа определены следующие режимы функционирования ИСПДн:
**штатный режим функционирования*, при котором клиентское, серверное программное обеспечение, технические средства пользователей и администратора системы обеспечивают возможность круглосуточного и ежедневного функционирования;
**аварийный режим функционирования*, при котором произошло нарушение функционирования одного или нескольких компонент программного и (или) технического обеспечения.

Резервное копирование ПДн в штатном режиме производится в соответствии Планом резервного копирования ПДн.

На протяжении периода времени, когда ИСПДн находится в аварийном состоянии, осуществляется ежедневное полное копирование, подлежащее резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

4.Учет и хранение резервных копий

Учету подлежат следующие типы носителей резервных копий:
*магнитооптические накопители;
*съемные диски;
*дисковые накопители.

4.1 Порядок учета резервных копий
Учет резервных копий, созданных автоматизированными средствами системы резервного копирования, производится в электронном журнале системы.
Резервные копии персональных данных маркируются следующим образом: <Название базы данных / каталога> _ <Дата и время резервной копии>.
Учет резервных копий, созданных вручную, осуществляется в Журнале восстановления, учета создания и использования резервных копий ПДн. с указанием даты, времени начала и окончания операций копирования или восстановления данных, а также с приведением комментариев в случае их необходимости. Также в Журнале резервного копирования учитывается:
создание копии по запросу;
полное копирование в случае возникновения аварийных ситуаций.
Форма Журнала представлена в Приложении 2 настоящего Регламента.
Ответственным за ведение Журнала является Администратор безопасности ИСПДн.

4.2 Порядок хранения резервных копий
Хранение носителей, содержащих ПДн, осуществляется в условиях, исключающих возможность хищения, изменения целостности или уничтожения содержащейся на них информации.
Носители резервных копий краткосрочного хранения хранятся в помещениях, доступ в которым ограничен.
Срок хранения резервных копий определяется согласно Плану резервного копирования. В случае необходимости долгосрочного хранения резервных копий по истечении 3 месяцев носители резервных копий перемещаются в сейфы, (металлические шкафы), запираемые на ключ или на отдельные сервера, для долгосрочного хранения, под ответственность Администратору безопасности ИСПДн.
Отметка о передаче носителей резервных копий для долгосрочного хранения резервных копий проставляется в Журнале восстановления, учета создания и использования резервных копий персональных данных.
Допускается повторное использование носителей резервных копий по истечении срока хранения ПДн.

5. Контроль резервного копирования

Машинные носители, предназначенные для долгосрочного хранения информации, периодически проверяются на их пригодность и отсутствие сбойных секторов.

При появлении сбойных секторов на машинных носителях информация с этих носителей переносится на исправные. Неисправные носители уничтожаются согласно Регламента по учету, хранению и уничтожению носителей персональных данных.

Контроль результатов всех процедур резервного копирования осуществляется Администратором безопасности ИСПДн. В случае обнаружения ошибки в процессе резервного копирования выполняется повторное резервное копирование.

Администратором безопасности ИСПДн несет ответственность за корректное ведение Журнала восстановления, учета создания и использования резервных копий персональных данных.

6. Восстановление персональных данных

Восстановление ПДн проводится в случае нарушения ее целостности вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок персонала, аппаратных сбоев и пр.

В случае необходимости восстановления ПДн из резервных копий Пользователь ИСПДн, который работает с этими данными, сообщает о случившемся своему руководителю.

Руководитель Пользователя ИСПДн оформляет запрос в форме служебной записки

или электронной заявки и направляет ее Администратору безопасности ИСПДн. В заявке должны быть указаны:
данные, которые необходимо восстановить;
дата и время, по состоянию на которые должны быть восстановлены данные;
желательный срок восстановления;
описание причины, по которой произошла потеря персональных данных
(ошибка пользователя, программный сбой и т.п.).

В зависимости от обстоятельств, по которым произошло нарушение целостности ПДн, Администратор безопасности ИСПДн принимает решение о необходимости полного или частичного восстановления потерянных данных.

Кроме того, Администратор безопасности ИСПДн, получив запрос на восстановление данных, принимает решение о реагировании на данный инцидент в соответствии с Регламентом по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности.

Администратор безопасности ИСПДн несет ответственность за восстановление утерянных данных. Восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более трех рабочих дней.

Факт восстановления ПДн регистрируется в Журнале восстановления, учета создания и использования резервных копий ПДн.

7.Пересмотр и внесение изменений

Пересмотр положений настоящего документа проводится в следующих случаях:
*на регулярной основе, но не реже одного раза в полгода;
*при появлении новых требований к обработке и обеспечению безопасности персональных данных со стороны российского законодательства и контролирующих органов исполнительной власти РФ;
*по результатам проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности ПДн;
*по результатам внутреннего контроля (аудита) системы защиты ПДн в случае выявления существенных нарушений;
*по результатам расследования инцидентов информационной безопасности,

связанных с обработкой и обеспечением безопасности ПДн и выявивших недостатки в правилах предоставления доступа ПДн.

Пересмотр и внесение изменений в настоящий документ регламентируется Регламентом по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности.

Ответственным за пересмотр настоящего Регламента является Администратор безопасности ИСПДн.

Внесение изменений производится на основании соответствующего приказа по ОО.

Приложение 1

Форма плана резервного копирования персональных данных

План резервного копирования персональных данных

Резервируемый массив данных	Периодичность копирования	Источник	Носитель резервной копии	Местоположение резервной копии	Метод резервного копирования	Способ создания резервных копий	Срок хранения копии
База данных «Работники», общие папки файл-сервера и т.п.	Ежедневная/ Ежемесячная	Work.bd.ru	Магнитная лента, съемный диск и т.п.	rezervcopy.ru, Сейф на 2-м этаже	Полное резервирование	Автоматический	

Приложение 2

Форма журнала восстановления, учета создания и использования резервных копий персональных данных

Журнал восстановления, учета создания и использования резервных копий персональных данных

Наименование	Дата и время начала	Дата и время завершения	Местоположение резервной копии	Ответственный	Тип копии	Метод создания копии	Место хранения копии

Приложение 6 к приказу
№ 35 от 03.03.2023

Акт оценки вреда
субъектам персональных данных
в КГБОУ «Новоалтайская общеобразовательная школа-интернат»

г. Новоалтайск «___» _____ 202__

Комиссия, действующая на основании приказа № ___ от _____202__ года «О создании комиссии по защите персональных данных», в составе председателя комиссии Некрасовой О.Н. и членов комиссии Соболевой И.Е., Киснер О.Г., Хаблак И.С., во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и приказа Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"» составила акт по результатам оценки вреда:

ОБРАЗЕЦ

№ п/п	Действия, которые осуществляет организация при обработке персональных данных	Степень вреда, который может быть причинен субъекту персональных данных при нарушении
1	Публикация персональных данных сотрудников на официальном сайте компании в виде Ф. И. О. и указания должности	Средняя
2	Обработка персональных данных, связанных с состоянием здоровья	Высокая
3	<…>	

Дата проведения оценки вреда: «____» _____ 202 __ года

Председатель комиссии:
директор школы-интерната _____ О.Н. Некрасова

Члены комиссии:
Главный бухгалтер _____ И.Е. Соболева
Заместитель директора по УВР _____ О.Г. Киснер
Инспектор по кадрам _____ И.С. Хаблак