ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ГУДЕРМЕССКАЯ СРЕДНЯЯ ШКОЛА
ИМ. УСМАНА АХМАРОВИЧА ОЗДАМИРОВА»
(ГБОУ «ГУДЕРМЕССКАЯ СШ ИМ. У.А. ОЗДАМИРОВА»)

УТВЕРЖДАЮ
Директор ГБОУ «Гудермесская СШ им. У.А. Оздамирова»
_____ М.С.Дакаев
«18» февраля 2026 г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 0090EC0C11F3304433E857E9D2EA9D4B7D
Владелец: ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "ГУДЕРМЕССКАЯ СРЕДНЯЯ ШКОЛА ИМ. УСМАНА АХМАРОВИЧА ОЗДАМИРОВА"
Действителен: с 24.02.2026 до 20.05.2027

Перечень мер по обеспечению безопасности персональных данных

г. Гудермес, 2026

1. Общие положения

1.1. Настоящий Перечень мер разработан в соответствии с:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» ;
- Приказом ФСТЭК России от 18.02.2013 № 21;
- Приказом Роскомнадзора от 05.09.2013 № 996;
- иными нормативными правовыми актами в области защиты персональных данных.

1.2. Настоящий документ определяет организационные, технические и программно-аппаратные меры, принимаемые Оператором для обеспечения безопасности персональных данных (Персональных данных) при их обработке в ГБОУ «Гудермесская СШ им. У.А. Оздамирова» (далее — Школа).

1.3. Ответственным за реализацию мер по обеспечению безопасности Персональных данных является заместитель директора по информационно-коммуникационным технологиям (ИКТ) Татиев Н.С. (назначен приказом директора от 18.02.2026 г. №16/1).

2. Организационные меры

2.1. Назначение ответственных лиц:

- Издан приказ о назначении лица, ответственного за обработку Персональных данных (Татиев Н.С.).
- Утверждён перечень должностей работников, имеющих доступ к Персональных данных.

2.2. Локальные нормативные акты:

- Утверждена Политика обработки персональных данных (размещена на сайте).
- Утверждено Положение об обработке персональных данных (внутренний документ).
- Утверждены формы согласий на обработку и распространение Персональных данных.
- Утверждена инструкция для сотрудников по работе с Персональных данных.

2.3. Организация работы с Персональных данных:

- Проведён инструктаж сотрудников, имеющих доступ к Персональных данных (под роспись).
- Определены места хранения материальных носителей Персональных данных (шкафы, сейфы, кабинеты).
- Обеспечено раздельное хранение Персональных данных, обрабатываемых в разных целях .

- Ведётся журнал учета согласий на обработку Персональных данных.
- Осуществляется контроль за действиями сотрудников с Персональных данных.

2.4. Работа с обращениями и инцидентами:

- Определён порядок рассмотрения обращений субъектов Персональных данных.
- Разработан порядок действий при утечке или утрате Персональных данных.

3. Меры при обработке Персональных данных без использования средств автоматизации (на бумажных носителях)

В соответствии с Постановлением Правительства РФ № 687 :

3.1. Определение мест хранения:

- Для каждой категории Персональных данных определены места хранения материальных носителей (личные дела сотрудников — в кадровом кабинете, личные дела обучающихся — в учебной части).

3.2. Раздельное хранение:

- Обеспечено раздельное хранение Персональных данных, обрабатываемых в различных целях (например, личные дела сотрудников и документы обучающихся хранятся отдельно).

3.3. Обеспечение сохранности:

- Документы на бумажных носителях хранятся в запирающихся металлических шкафах/сейфах.
- Помещения, в которых хранятся Персональных данных, оборудованы замками, сигнализацией, имеют пропускной режим.
- Ключи от шкафов и помещений хранятся у ответственных лиц.

3.4. Контроль доступа:

- Установлен перечень лиц, имеющих доступ к бумажным носителям Персональных данных.
- Выдача документов третьим лицам осуществляется только на основании письменного запроса и с разрешения директора.

4. Меры при обработке Персональных данных с использованием средств автоматизации (в электронном виде)

4.1. Защита информации при обработке в ИСПерсональных данных:

- Учёт машин-носителей и пользователей информационной системы.
- Применение парольной защиты доступа к ПК и информационным системам (электронный журнал «Дневник.ру», бухгалтерская программа, локальные базы данных).

4.2. Антивирусная защита:

- На всех компьютерах, используемых для обработки Персональных данных, установлено лицензионное антивирусное программное обеспечение.
- Обеспечено регулярное обновление антивирусных баз.

4.3. Защита сети и каналов связи:

- Использование межсетевых экранов (брандмауэров).
- При передаче Персональных данных по сети Интернет (например, при отправке отчётности) используется шифрование (TLS/HTTPS).

4.4. Резервное копирование:

- Регулярное создание резервных копий баз данных, содержащих Персональных данных.
- Хранение резервных копий в защищённом месте.

4.5. Контроль доступа к электронным носителям:

- Разграничение прав доступа пользователей к информационным системам.
- Использование учётных записей для каждого сотрудника.
- Отключение неиспользуемых учётных записей.

5. Меры по защите информации при передаче Персональных данных

5.1. При передаче Персональных данных по внутренним каналам связи используются средства шифрования.

5.2. При направлении Персональных данных по электронной почте:

- Используются защищённые каналы связи (TLS).
- Запрещена отправка Персональных данных на личные почтовые ящики сотрудников (только на корпоративные).

5.3. При передаче Персональных данных внешним организациям (РКН, ПФР, налоговая, органы опеки и т.д.):

- Передача осуществляется по защищённым каналам или на бумажных носителях с курьером.

6. Контроль доступа и пропускной режим

6.1. В помещения, где обрабатываются и хранятся Персональных данных (кадровый кабинет, бухгалтерия, учебная часть, кабинет ИКТ), доступ посторонних лиц ограничен.

6.2. В Школе организован пропускной режим:

- Установлена система контроля доступа (СКУД) или запирающиеся двери.
- Ведётся журнал учёта посетителей.

6.3. В кабинетах, где ведётся обработка Персональных данных с использованием ПК, экраны мониторов развёрнуты таким образом, чтобы исключить просмотр информации посторонними лицами.

7. Контроль эффективности принятых мер

7.1. Внутренний контроль:

- Ежеквартальная проверка соблюдения требований безопасности Персональных данных ответственным лицом (Татиев Н.С.).
- Проверка ведения журналов и наличия согласий.

7.2. Внешний контроль:

- Готовность к проверкам Роскомнадзора (РКН).
- Предоставление отчётности и сведений в уполномоченные органы по запросу.

7.3. Реагирование на инциденты:

- При обнаружении факта утечки или утраты Персональных данных — немедленное уведомление РКН в порядке, установленном законодательством.

8. Заключительные положения

8.1. Все сотрудники Школы, имеющие доступ к Персональных данных, ознакомлены с настоящим Перечнем мер под роспись.

8.2. Изменения в Перечень мер вносятся приказом директора по представлению ответственного за Персональных данных (Татиев Н.С.).

8.3. Контроль за исполнением Перечня мер возлагается на заместителя директора по ИКТ Татиева Н.С.