

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 3
С. ГОЙТЫ ИМЕНИ Р. АРСАНУКАЕВА»
(МБОУ «СОШ № 3 с. Гойты им. Р. Арсанукаева»)**

ПРИНЯТО

на заседании педагогического совета
Протокол № 1 от «28» августа 2026 г.

УТВЕРЖДАЮ

директор
МБОУ «СОШ № 3 с. им. Р. Арсанукаева»
_____/ М.Х. Магомадова /
от 29.08.2026 №97-од

ПОЛОЖЕНИЕ

о защите информации в МБОУ «СОШ №3 с. Гойты им. Р. Арсанукаева»

1. Общие положения

1.1. Настоящее Положение о защите информации (далее – Положение) является локальным нормативным актом МБОУ «СОШ №3 с. Гойты им. Р. Арсанукаева» (далее – Школа) и устанавливает единые цели, принципы, организационные основы и порядок обеспечения защиты информации, обрабатываемой в информационных системах Школы, с учётом требований нормативных правовых актов Российской Федерации.

1.2. Настоящее Положение разработано в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в ред. от 29.12.2025);
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (в ред. от 26.07.2026 № 265-ФЗ);
- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (в ред. от 04.08.2026);
- приказом ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (в ред. от 08.05.2026, действует с 01.03.2026);
- постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСТЭК России от 11.04.2025 № 117 (ред. от 08.05.2026);
- методическими рекомендациями Минпросвещения России от 10.11.2025 № ИШ-2224/04 по обеспечению оптимальным и безопасным доступом к информационным системам и сети «Интернет»;
- постановлением Правительства РФ от 06.05.2026 № 517 (изменения в правила применения электронного обучения и дистанционных образовательных технологий, действуют с 15.05.2026);
- Уставом МБОУ «СОШ №3 с. Гойты им. Р. Арсанукаева»;

- иными нормативными правовыми актами, регулирующими отношения в сфере защиты информации и персональных данных.
- 1.3. Настоящее Положение является Политикой защиты информации Школы в соответствии с требованиями приказа ФСТЭК России № 117.
- 1.4. Положение распространяется на все информационные системы Школы, в которых обрабатывается защищаемая информация, включая государственные и муниципальные информационные системы, а также иные информационные системы Школы (бухгалтерские, кадровые, автоматизированные системы управления, образовательные платформы).
- 1.5. Целью защиты информации в Школе является предотвращение событий, приводящих к негативным последствиям, в том числе к утечке персональных данных, нарушению функционирования информационных систем, материальному ущербу.
- 1.6. С 1 марта 2026 года вступили в силу обновлённые Требования о защите информации, утверждённые приказом ФСТЭК России от 11.04.2025 № 117. Приказ ФСТЭК России от 11.02.2013 № 17 признан утратившим силу. Аттестаты соответствия, выданные до 1 марта 2026 года, считаются действительными.

2. Основные понятия и определения

2.1. В настоящем Положении используются следующие понятия:

- **Информация** – сведения (сообщения, данные) независимо от формы их представления;
- **Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;
- **Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств;
- **Защита информации** – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;
- **Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя;
- **Целостность информации** – состояние информации, при котором отсутствует любое её изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- **Доступность информации** – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;
- **Несанкционированный доступ** – доступ к информации или действия с информацией, осуществляемые субъектом, не имеющим права доступа к этой информации;
- **Утечка информации** – неконтролируемое распространение защищаемой информации, её разглашение, а также несанкционированный доступ к ней.

3. Цели и задачи защиты информации

3.1. Основными целями защиты информации в Школе являются:

- обеспечение конфиденциальности, целостности и доступности защищаемой информации;
- предотвращение неправомерного доступа к информации, её уничтожения, искажения, блокирования;
- защита прав и законных интересов субъектов персональных данных;
- обеспечение безопасности образовательного процесса и функционирования информационной инфраструктуры Школы;
- соблюдение требований законодательства Российской Федерации в области защиты информации.

3.2. Основными задачами защиты информации являются:

- выявление и предотвращение угроз информационной безопасности;
- создание и поддержание функционирования системы защиты информации;
- организация и осуществление контроля за соблюдением требований по защите информации;
- своевременное выявление и реагирование на инциденты информационной безопасности;
- повышение уровня осведомлённости работников Школы в области информационной безопасности.

4. Объекты защиты информации

4.1. Объектами защиты информации в Школе являются:

- информация, обрабатываемая в информационных системах Школы, включая персональные данные работников, обучающихся и их законных представителей;
- информационные ресурсы Школы, включая базы данных, файловые хранилища, электронные документы;
- информационно-технологическая инфраструктура, включая серверы, рабочие станции, сетевое оборудование, каналы связи;
- системы и подсистемы защиты информации Школы;
- помещения, в которых размещены технические средства обработки информации.

5. Принципы защиты информации

5.1. Защита информации в Школе осуществляется на основе следующих принципов:

- **законность** – соответствие мер защиты информации требованиям законодательства Российской Федерации;
- **системность** – комплексное применение мер защиты на всех этапах обработки информации;
- **своевременность** – принятие мер защиты до момента возникновения угрозы;
- **непрерывность** – постоянное функционирование системы защиты информации;
- **разграничение доступа** – предоставление доступа к информации только уполномоченным лицам;
- **персональная ответственность** – закрепление ответственности за обеспечение защиты информации за конкретными работниками;
- **экономическая целесообразность** – соразмерность затрат на защиту информации возможному ущербу.

6. Организационные меры защиты информации

6.1. Организационные меры защиты информации включают:

- назначение ответственного за обеспечение защиты информации в Школе приказом директора;
- разработку и утверждение локальных нормативных актов по защите информации;
- определение перечня защищаемой информации и категорий доступа к ней;
- разграничение прав доступа работников к информации и информационным системам;
- организацию учёта носителей защищаемой информации;
- проведение инструктажей и обучение работников по вопросам защиты информации;
- организацию контроля за соблюдением требований по защите информации;
- организацию учёта инцидентов информационной безопасности и реагирования на них.

6.2. Ответственный за обеспечение защиты информации назначается приказом директора Школы из числа заместителей директора или иных уполномоченных лиц.

6.3. Перечень должностей, замещение которых предусматривает обработку защищаемой информации или доступ к ней, утверждается приказом директора Школы.

7. Технические меры защиты информации

7.1. Технические меры защиты информации включают:

- применение антивирусного программного обеспечения;
- применение средств криптографической защиты информации (СКЗИ) при передаче данных по каналам связи;
- использование межсетевых экранов и систем обнаружения вторжений;
- разграничение прав доступа к информационным ресурсам;
- резервное копирование данных;
- ведение электронных журналов безопасности;
- применение парольной защиты;
- организацию безопасного подключения к сети «Интернет»;
- использование аттестованных рабочих мест для работы с конфиденциальной информацией.

7.2. Криптографическая защита информации осуществляется в соответствии с требованиями:

- Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств (утв. постановлением Правительства РФ от 16.04.2012 № 313);
- ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры»;
- ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры»;
- ГОСТ 34.13-2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».

7.3. При осуществлении передачи данных для доступа к государственным, муниципальным и иным информационным системам, в которых осуществляется обработка персональных данных, обеспечивается криптографическая защита

информации в соответствии с методическими рекомендациями Минпросвещения России от 10.11.2025 № ИШ-2224/04.

8. Защита информации при использовании дистанционных образовательных технологий

8.1. С 15 мая 2026 года вступили в силу изменения в правила применения электронного обучения и дистанционных образовательных технологий (постановление Правительства РФ от 06.05.2026 № 517).

8.2. Для организации взаимодействия участников образовательных отношений в рамках электронного или дистанционного обучения в обязательном порядке применяется многофункциональный сервис обмена информацией — мессенджер МАХ, интегрированный во ФГИС «Моя школа».

8.3. Использование сторонних коммерческих платформ и несертифицированных сервисов для передачи персональных данных обучающихся находится под строгим запретом.

8.4. При использовании систем прокторинга (контроля честности дистанционных испытаний) обеспечивается защита персональных данных и соблюдение требований законодательства.

9. Защита персональных данных

9.1. Защита персональных данных осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (в ред. от 26.07.2026 № 265-ФЗ) и принятыми в соответствии с ним нормативными правовыми актами.

9.2. В 2026 году ужесточены требования к защите персональных данных:

- обязательная регистрация операторов в реестре Роскомнадзора;
- локализация баз данных на территории Российской Федерации;
- оформление согласия на обработку персональных данных как отдельного документа;
- принцип минимизации — сбор только тех данных, которые необходимы для конкретной цели;
- для обработки биометрических и специальных данных требуется отдельное согласие и повышенные меры защиты.

9.3. Защита персональных данных осуществляется в соответствии с отдельным локальным нормативным актом Школы — **Положением об обработке и защите персональных данных**.

10. Права и обязанности работников в области защиты информации

10.1. Работники Школы обязаны:

- соблюдать требования законодательства Российской Федерации и локальных нормативных актов Школы в области защиты информации;
- не разглашать защищаемую информацию, ставшую известной в связи с исполнением должностных обязанностей;
- соблюдать правила работы с информационными системами и носителями информации;
- незамедлительно сообщать ответственному за защиту информации о фактах нарушения режима защиты информации;
- проходить обучение и инструктажи по вопросам защиты информации.

10.2. Работники Школы имеют право:

- на получение информации о требованиях по защите информации;
- на ознакомление с локальными нормативными актами, регуливающими защиту информации;
- на обращение к руководству Школы по вопросам обеспечения защиты информации.

11. Ответственность за нарушение требований по защите информации

11.1. Работники Школы, виновные в нарушении требований по защите информации, несут дисциплинарную, материальную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

11.2. **Административная ответственность** за нарушение требований по защите информации установлена статьями 13.11, 13.11.1, 13.12, 13.13, 13.14 КоАП РФ.

11.3. **Уголовная ответственность** предусмотрена статьями 272, 273, 274, 274.1 УК РФ за неправомерный доступ к компьютерной информации, создание и распространение вредоносных программ, нарушение правил эксплуатации средств хранения и обработки информации.

11.4. В 2026 году увеличены штрафы за нарушения в области защиты информации:

- за обработку персональных данных без согласия субъекта — до **700 000 рублей**;
- за невыполнение обязанности по опубликованию политики — до **60 000 рублей**;
- за нарушение требований по обезличиванию — до **500 000 рублей**.

12. Контроль за обеспечением защиты информации

12.1. Контроль за обеспечением защиты информации в Школе осуществляется:

- директором Школы;
- ответственным за обеспечение защиты информации;
- комиссией по защите информации (при необходимости).

12.2. Формы контроля:

- плановые и внеплановые проверки соблюдения требований по защите информации;
- анализ журналов безопасности и инцидентов;
- оценка эффективности применяемых мер защиты;
- проведение аудита информационной безопасности.

12.3. Результаты контроля оформляются актом (справкой) и рассматриваются на совещании при директоре.

13. Заключительные положения

13.1. Настоящее Положение вступает в силу с момента его утверждения приказом директора Школы и действует до принятия нового Положения.

13.2. Изменения и дополнения в настоящее Положение вносятся в порядке, установленном Трудовым кодексом Российской Федерации и локальными нормативными актами Школы.

13.3. Настоящее Положение подлежит пересмотру **не реже одного раза в год**, а также при изменении законодательства Российской Федерации, регулирующего вопросы защиты информации.

13.4. Действие настоящего Положения сохраняется до **1 марта 2031 года** — в пределах срока действия приказа ФСТЭК России от 11.04.2025 № 117 (с учётом возможных изменений).

13.5. Контроль за исполнением настоящего Положения возлагается на директора Школы.

Приложение №1
к Положению о защите информации
МБОУ «СОШ №3 с. Гойты им. Р. Арсанукаева»

Перечень защищаемой информации

№ п/п	Категория информации	Состав информации
1	Персональные данные работников	Ф.И.О., паспортные данные, СНИЛС, ИНН, адрес, контактные данные, сведения об образовании, банковские реквизиты
2	Персональные данные обучающихся	Ф.И.О., дата рождения, адрес, контактные данные, сведения об успеваемости, медицинские показания
3	Персональные данные родителей (законных представителей)	Ф.И.О., контактные данные, паспортные данные
4	Учебная и методическая информация	Рабочие программы, учебные планы, методические материалы, контрольно-измерительные материалы
5	Финансово-хозяйственная информация	Бухгалтерская отчётность, договоры, сметы, планы финансово-хозяйственной деятельности
6	Управленческая информация	Приказы, распоряжения, протоколы совещаний, служебная переписка
7	Информация о системе защиты информации	Пароли, ключи доступа, журналы безопасности, конфигурации систем защиты

Приложение №2
к Положению о защите информации
МБОУ «СОШ №3 с. Гойты им. Р. Арсанукаева»

Лист ознакомления с Положением о защите информации

С Положением о защите информации ознакомлен (а):

№ п/п	Фамилия, имя, отчество работника	Должность	Дата и подпись работника после ознакомления с Положением

Приложение №3
к Положению о защите информации
МБОУ «СОШ №3 с. Гойты им. Р. Арсанукаева»

**Перечень должностей, замещение которых предусматривает обработку
защищаемой информации**

УТВЕРЖДЁН

приказом директора

МБОУ «СОШ №3 с. Гойты им. Р. Арсанукаева»

от «___» _____ 2026 г. № ___

№ п/п	Наименование должности	Категория доступа к защищаемой информации
1	Директор	Полный доступ
2	Заместитель директора по УР	Доступ к персональным данным обучающихся, учебной информации
3	Заместитель директора по ВР	Доступ к персональным данным обучающихся, воспитательной информации
4	Заместитель директора по АХР	Доступ к финансово-хозяйственной информации
5	Главный бухгалтер	Доступ к финансово-хозяйственной информации, персональным данным работников
6	Специалист по кадрам	Доступ к персональным данным работников
7	Секретарь учебной части	Доступ к персональным данным обучающихся, управленческой информации
8	Системный администратор	Доступ к информационным системам, системе защиты информации
9	Педагогические работники	Доступ к персональным данным обучающихся, учебной информации

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00BAEA890E7DFB534CB1FC1DE0AAE96A0C
Владелец: Магомадова Мадина Хасановна
Действителен: с 31.10.2025 до 24.01.2027