**Муниципальное общеобразовательное бюджетное учреждение средняя общеобразовательная школа с. Мирный муниципального района Благоварский район Республики Башкортостан (МОБУ СОШ с. Мирный)**

**УТВЕРЖДЕНА**
приказом директора
МОБУ СОШ с. Мирный
от 30.09.2026 №203-ОД

**РАССМОТРЕНА**
Управляющим советом
Протокол от 29.09.2026 №2

*Подлежит размещению в неограниченном доступе на официальном сайте Школы*

# ПОЛИТИКА ЗАЩИТЫ ИНФОРМАЦИИ МОБУ СОШ с. Мирный

## 1. Общие положения

1.1. Настоящая Политика защиты информации (далее – Политика) Муниципального общеобразовательного бюджетного учреждения средняя общеобразовательная школа с. Мирный муниципального района Благоварский район Республики Башкортостан (далее – Школа) определяет цели, задачи, принципы и правила обеспечения защиты информации в Школе, а также устанавливает совокупность организационных и технических мер, направленных на обеспечение информационной безопасности (далее – ИБ) при осуществлении уставной деятельности Школы.

1.2. Политика разработана в соответствии со следующими нормативными правовыми актами:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Приказ 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»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Минпросвещения России от 30.04.2021 № 221 «Об утверждении требований к подключению и доступу… к единой сети передачи данных»;
- Устав МОБУ СОШ с. Мирный.

1.3. Политика является основополагающим документом системы обеспечения ИБ

Школы и обязательна для исполнения всеми работниками Школы, а также иными лицами, получающими доступ к информационным системам и информационно-телекоммуникационной инфраструктуре Школы.

1.4. На основе Политики в Школе разрабатываются внутренние стандарты и регламенты по защите информации, инструкции пользователей и иные организационно-распорядительные документы в области ИБ.

1.5. Ответственность за обеспечение защиты информации в Школе несёт директор Школы. Непосредственное обеспечение ИБ осуществляется работником, назначенным приказом директора Школы ответственным за обеспечение защиты информации (далее — Ответственный за ИБ).

1.6. Политика пересматривается не реже одного раза в три года, а также при существенных изменениях в законодательстве, структуре информационных систем или инфраструктуре Школы.

## 2. Область действия политики

2.1. Действие Политики распространяется на все информационные системы (далее — ИС), компоненты информационно-телекоммуникационной инфраструктуры (далее — ИТИ) и информацию, обрабатываемую в Школе, включая:

2.1.1. Информационные системы Школы:

- ФГИС «Моя школа» (электронный журнал/дневник);
- ФИС ОКО (Федеральная информационная система оценки качества образования);
- ФИС ФРДО (Федеральный реестр сведений о документах об образовании);
- Сайт Школы (официальный);
- Информационная система персональных данных (ИСПДн) Школы;
- Локальные информационные системы, используемые в административно-хозяйственной деятельности.

2.1.2. Информационно-телекоммуникационную инфраструктуру:

- Локальная вычислительная сеть (ЛВС) Школы;
- Рабочие станции, ноутбуки, планшеты, интерактивные доски, принтеры, МФУ;
- Сетевое оборудование (коммутаторы, маршрутизаторы, точки доступа Wi-Fi);
- Подключение к сети «Интернет» через Единую сеть передачи данных (ЕСПД), организованное ПАО «Ростелеком»;
- Средства защиты информации (антивирусное ПО, межсетевые экраны, средства криптографической защиты).

2.1.3. Информацию, обрабатываемую в Школе:

- Персональные данные обучающихся, их родителей (законных представителей), работников Школы;
- Сведения ограниченного доступа (служебная информация, информация, содержащаяся в ИС ограниченного доступа);
- Информацию, доступ к которой ограничен в соответствии с законодательством Российской Федерации.

2.2. Действие Политики распространяется на всех работников Школы (штатных, внештатных, работающих по совместительству), обучающихся, а также иных лиц (подрядные организации, специалисты сервисного обслуживания), получающих доступ к ИС и ИТИ Школы.

## 3. Цели и задачи защиты информации

3.1. **Цели защиты информации**

3.1.1. Исключение утечки информации ограниченного доступа и иной конфиденциальной информации, в том числе персональных данных.

3.1.2. Предотвращение несанкционированного доступа (далее – НСД) к ИС и содержащейся в них информации, обнаружение фактов НСД и реагирование на них.

3.1.3. Предотвращение несанкционированной модификации, подмены и удаления информации и программного обеспечения, обнаружение фактов такого воздействия и реагирование на них.

3.1.4. Исключение или существенное затруднение отказа в обслуживании авторизованным пользователям ИС.

3.1.5. Недопущение использования ИС и содержащейся в них информации не по назначению.

3.1.6. Исключение или существенное затруднение нарушения функционирования (работоспособности) ИС.

3.1.7. Недопущение распространения с использованием ИС противоправной информации, в том числе информации, причиняющей вред здоровью и (или) развитию детей.

3.1.8. Обеспечение возможности восстановления доступа авторизованных пользователей к ИС и информации в установленные сроки.

3.1.9. Обеспечение возможности восстановления информации, модифицированной или уничтожённой вследствие реализации угроз безопасности информации.

3.2. **Задачи защиты информации**

3.2.1. Разработка и поддержание в актуальном состоянии организационно-распорядительных документов в области ИБ (Политики, внутренних стандартов, регламентов, инструкций).

3.2.2. Идентификация и аутентификация пользователей ИС, управление учётными записями и правами доступа.

3.2.3. Обеспечение защиты информации при обработке, хранении и передаче, в том числе при удалённом доступе и доступе через сеть «Интернет».

3.2.4. Организация антивирусной защиты, защиты от сетевых атак и вредоносного кода.

3.2.5. Управление уязвимостями и обновлениями программного обеспечения.

3.2.6. Обеспечение непрерывности функционирования ИС и резервного копирования данных.

3.2.7. Организация мониторинга событий безопасности и реагирования на инциденты ИБ.

3.2.8. Организация обучения работников Школы по вопросам ИБ и проверка их знаний.

3.2.9. Контроль уровня защищённости информации (расчёт показателей Кзи и Пзи).

3.2.10. Защита обучающихся от информации, причиняющей вред их здоровью и (или) развитию, при использовании сети «Интернет».

## 4. Принципы защиты информации

4.1. Законность – обеспечение защиты информации в соответствии с требованиями законодательства Российской Федерации.

4.2. Системность – комплексное применение организационных и технических мер защиты, охватывающих все ИС, компоненты ИТИ и процессы обработки информации.

4.3. Непрерывность – постоянное обеспечение защиты информации на всех этапах жизненного цикла ИС.

4.4. Адекватность – соответствие мер защиты актуальным угрозам и уровню критичности защищаемой информации.

4.5. Минимально необходимый доступ – предоставление пользователям только тех прав доступа, которые необходимы для выполнения служебных (учебных) обязанностей.

4.6. Разделение полномочий – распределение функций по обеспечению ИБ между различными работниками с целью исключения конфликта интересов.

4.7. Контролируемость – обеспечение возможности контроля эффективности применяемых мер защиты и соблюдения установленных требований.

4.8. Персональная ответственность – каждый работник Школы несёт персональную ответственность за соблюдение требований ИБ в пределах своих полномочий.

4.9. Приоритет защиты обучающихся – обеспечение безопасного доступа обучающихся к сети «Интернет» через ЕСПД с контентной фильтрацией.

## 5. Объекты защиты

5.1. **Информационные активы**

К защищаемым информационным активам Школы относятся:

5.1.1. Персональные данные обучающихся, родителей (законных представителей) и работников Школы: фамилия, имя, отчество, дата рождения, адрес, сведения об образовании, месте работы, должности, доходах и иные сведения, относимые к персональным данным в соответствии с Федеральным законом № 152-ФЗ.

5.1.2. Сведения, составляющие служебную тайну и информацию ограниченного доступа: приказы по личному составу, материалы аттестации работников, результаты внутренней оценки качества образования, финансово-экономическая документация.

5.1.3. Учебно-методические материалы, рабочие программы, контрольно-измерительные материалы, иные материалы, доступ к которым ограничен решением директора Школы.

5.1.4. Информация, запрещённая для распространения среди детей в соответствии с Федеральным законом № 436-ФЗ.

5.2. **Программные и программно-аппаратные средства**

5.2.1. Серверное оборудование и операционные системы серверов.

5.2.2. Рабочие станции, ноутбуки, планшеты, интерактивные доски.

5.2.3. Сетевое оборудование (коммутаторы, маршрутизаторы, точки доступа Wi-Fi).

5.2.4. Средства защиты информации (антивирусное ПО, межсетевые экраны, средства криптографической защиты информации).

5.2.5. Прикладное программное обеспечение (электронный журнал, бухгалтерские программы, системы документооборота).

5.3. **Информационные системы**

5.3.1. ИСПДн Школы (информационная система персональных данных).

5.3.2. ФГИС «Моя школа».

5.3.3. ФИС ОКО, ФИС ФРДО.

5.3.4. Официальный сайт Школы.

5.3.5. Иные ИС, эксплуатируемые в Школе.

5.4. **Сети и подсети**

5.4.1. Локальная вычислительная сеть Школы.

5.4.2. Подключение к ЕСПД (канал передачи данных, организованный ПАО «Ростелеком»).

5.4.3. Беспроводные сети Wi-Fi (при наличии).

## 6. Категории лиц, участвующих в защите информации, их обязанности и полномочия

6.1. **Директор Школы**

6.1.1. Осуществляет общее руководство деятельностью по обеспечению защиты информации в Школе.

6.1.2. Утверждает Политику, внутренние стандарты и регламенты по защите информации.

6.1.3. Назначает приказом Ответственного за ИБ и определяет его обязанности.

6.1.4. Выделяет организационные, технические и иные ресурсы, необходимые для обеспечения защиты информации.

6.1.5. Принимает решения по результатам оценки показателей защищённости (Кзи и Пзи) и плану мероприятий по повышению уровня защищённости.

6.1.6. Рассматривает результаты внутреннего контроля соблюдения требований ИБ.

6.2. **Ответственный за обеспечение защиты информации**

6.2.1. Разрабатывает и поддерживает в актуальном состоянии Политику, внутренние стандарты и регламенты по защите информации.

6.2.2. Осуществляет идентификацию и аутентификацию пользователей, управление учётными записями и правами доступа.

6.2.3. Обеспечивает установку, настройку и обновление средств защиты информации.

6.2.4. Организует антивирусную защиту, защиту от сетевых атак и вредоносного кода.

6.2.5. Обеспечивает управление уязвимостями и обновлениями программного обеспечения.

6.2.6. Организует резервное копирование данных и контроль его выполнения.

6.2.7. Осуществляет мониторинг событий безопасности, выявление и регистрацию инцидентов ИБ.

6.2.8. Организует обучение работников Школы по вопросам ИБ и проверку их знаний.

6.2.9. Проводит оценку показателей защищённости (Кзи – не реже 1 раза в 6 месяцев, Пзи – не реже 1 раза в 2 года).

6.2.10. Направляет результаты оценки показателей в ФСТЭК России в установленные сроки.

6.2.11. Взаимодействует с подразделением ГосСОПКА, органами управления образованием, оператором ЕСПД (ПАО «Ростелеком») по вопросам ИБ.

6.2.12. Контролирует соблюдение работниками Школы требований Политики и внутренних документов по ИБ.

6.3. **Работники Школы (пользователи ИС)**

6.3.1. Соблюдают требования Политики и внутренних документов по ИБ.

6.3.2. Используют ИС и средства доступа только в служебных целях.

6.3.3. Обеспечивают сохранность учётных данных (логинов, паролей, токенов) и не передают их третьим лицам.

6.3.4. Не устанавливают нелицензионное и не согласованное с Ответственным за ИБ

программное обеспечение.

6.3.5. Не подключают личные съёмные носители к рабочим станциям без проверки на вредоносное ПО.

6.3.6. Неотлагательно сообщают Ответственному за ИБ о подозрениях на нарушение ИБ, обнаружении вредоносного ПО, подозрительных письмах (фишинге), попытках несанкционированного доступа.

6.3.7. Не разглашают конфиденциальную информацию и персональные данные третьим лицам.

6.3.8. Проходят обучение по вопросам ИБ и проверку знаний в установленные сроки.

6.4. **Обучающиеся**

6.4.1. Используют сеть «Интернет» через ЕСПД только в учебных целях под контролем педагогических работников.

6.4.2. Соблюдают правила безопасного поведения в сети «Интернет».

6.4.3. Не предпринимают действий, направленных на нарушение работы ИС и средств защиты информации.

6.5. **Подрядные организации и специалисты сервисного обслуживания**

6.5.1. Допуск к ИС и ИТИ Школы осуществляется на основании договора и приказа директора Школы.

6.5.2. Подрядные организации обязаны соблюдать требования Политики в части, их касающейся, что должно быть закреплено в договоре.

6.5.3. Доступ подрядных организаций предоставляется на ограниченный срок и по завершении работ – прекращается.

## 7. Состав организационной системы управления деятельностью по защите информации и схема взаимодействия её элементов

7.1. **Структура системы управления ИБ**

7.1.1. Управление деятельностью по защите информации в Школе осуществляется на трёх уровнях:

Уровень 1 – стратегический (директор Школы):

• Общее руководство, утверждение документов, выделение ресурсов, принятие решений по результатам оценки защищённости.

Уровень 2 – организационно-технический (Ответственный за ИБ):

• Разработка и реализация мер защиты, контроль исполнения, мониторинг, обучение, оценка показателей защищённости.

Уровень 3 – исполнительный (работники Школы – пользователи ИС):

• Соблюдение требований ИБ в повседневной деятельности, информирование об инцидентах.

7.2. **Внутренние документы системы ИБ**

7.2.1. Система управления ИБ Школы включает следующие документы:

- Политика защиты информации (настоящий документ);
- Внутренние стандарты по защите информации;
- Внутренние регламенты по защите информации (16 регламентов);
- Инструкции пользователей по ИБ;
- Модель угроз безопасности информации;
- Акт классификации ИСПДн;
- Приказы директора по вопросам ИБ.

7.3. **Перечень внутренних регламентов по защите информации**

7.3.1. В Школе утверждены и действуют следующие внутренние регламенты:

1) Регламент управления учётными записями пользователей ИС;
2) Регламент управления привилегированными учётными записями;
3) Регламент управления аутентификационной информацией и средствами аутентификации;
4) Регламент предоставления удалённого доступа к ИС;
5) Регламент доступа пользователей ИС в сеть «Интернет» через ЕСПД;
6) Регламент обучения пользователей по вопросам ИБ и проверки знаний;
7) Регламент управления уязвимостями ИС;
8) Регламент управления обновлениями программного обеспечения;
9) Регламент защиты информации ограниченного доступа;
10) Регламент физической защиты объектов ИТИ;
11) Регламент мониторинга событий безопасности;
12) Регламент реагирования на инциденты ИБ;
13) Регламент резервного копирования информации, ПО и конфигураций;
14) Регламент контроля уровня защищённости информации (Кзи и Пзи);
15) Регламент работы со съёмными носителями информации;
16) Регламент доступа работников подрядных организаций к ИС.

7.4. **Взаимодействие с внешними организациями**

7.4.1. Школа взаимодействует со следующими внешними организациями по вопросам ИБ:

- ФСТЭК России – направление результатов оценки показателей защищённости (Кзи и Пзи);
- Роскомнадзор – уведомления об обработке персональных данных, реагирование на обращения;
- НКЦКИ (ГосСОПКА) – информирование о компьютерных инцидентах;
- ПАО «Ростелеком» (оператор ЕСПД) – техническая поддержка, вопросы контентной фильтрации, доступ к сети «Интернет»;
- Управление образования администрации муниципального района – организационно-методическое руководство.

## 8. Ответственность работников за нарушение требований о защите информации и установленных правил обработки информации

8.1. Работники Школы несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность за нарушение требований о защите информации в соответствии с законодательством Российской Федерации.

8.2. Дисциплинарная ответственность применяется за нарушение требований Политики и внутренних документов по ИБ в виде замечания, выговора или увольнения в соответствии с трудовым законодательством.

8.3. Административная ответственность наступает за нарушение правил обработки персональных данных (статья 13.11 КоАП РФ), нарушение требований защиты информации (статья 13.12 КоАП РФ) и иные правонарушения в области информации.

8.4. Уголовная ответственность наступает за неправомерный доступ к компьютерной информации (статья 272 УК РФ), создание, использование и распространение вредоносных программ (статья 273 УК РФ), нарушение правил эксплуатации средств хранения,

обработки или передачи компьютерной информации (статья 274 УК РФ).

8.5. Ответственный за ИБ несёт ответственность за ненадлежащее исполнение возложенных на него обязанностей по обеспечению защиты информации.

8.6. Обучающиеся несут дисциплинарную ответственность за нарушение правил работы в ИС Школы и правил безопасного поведения в сети «Интернет» в соответствии с Уставом Школы и локальными актами.

8.7. Подрядные организации несут ответственность за нарушение требований Политики в соответствии с условиями договора.

## 9. Требования по информационной безопасности

9.1. **Управление доступом**

9.1.1. Доступ к ИС Школы предоставляется на основе идентификации и аутентификации пользователей с применением паролей или иных средств аутентификации.

9.1.2. Парольная политика: минимальная длина пароля — не менее 12 символов; обязательное использование строчных и заглавных букв, цифр и специальных символов; срок действия пароля — не более 90 дней; запрет повторного использования последних 5 паролей; блокировка учётной записи после 5 неудачных попыток входа.

9.1.3. Для привилегированных учётных записей (администраторов) применяется многофакторная аутентификация.

9.1.4. Учётные записи создаются, изменяются, блокируются и удаляются в порядке, установленном Регламентом управления учётными записями. Запрещено использование сервисных учётных записей с паролями по умолчанию.

9.1.5. При увольнении работника его учётные записи блокируются в день увольнения.

9.2. **Защита информации при работе в сети «Интернет» через ЕСПД**

9.2.1. Доступ Школы к сети «Интернет» осуществляется исключительно через ЕСПД, организованную ПАО «Ростелеком».

9.2.2. Контентная фильтрация осуществляется на стороне ЕСПД. Школа обеспечивает контроль использования сети «Интернет» обучающимися и работниками.

9.2.3. Запрещается использование альтернативных каналов доступа к сети «Интернет» (модемы, мобильные точки доступа, сторонние провайдеры) на рабочих станциях, подключённых к ЛВС Школы.

9.2.4. Разблокировка образовательных ресурсов, ошибочно заблокированных контентной фильтрацией ЕСПД, осуществляется через обращение в техническую поддержку ЕСПД или личный кабинет оператора.

9.2.5. Доступ обучающихся к сети «Интернет» осуществляется только под контролем педагогического работника.

9.3. **Антивирусная защита**

9.3.1. На всех рабочих станциях, серверах и ноутбуках Школы должно быть установлено и активно антивирусное программное обеспечение с актуальными базами сигнатур.

9.3.2. Запрещается отключение, блокировка или изменение настроек антивирусного ПО без разрешения Ответственного за ИБ.

9.3.3. Все съёмные носители должны быть проверены антивирусным ПО перед использованием.

9.3.4. Входящий трафик проверяется средствами антивирусной защиты, встроенными в контентную фильтрацию ЕСПД.

9.4. **Защита от несанкционированного доступа**

9.4.1. Доступ к серверному оборудованию ограничен. Помещение для размещения серверов должно быть запираемым.

9.4.2. Рабочие станции, оставляемые без присмотра, должны быть заблокированы (блокировка экрана) или выключены.

9.4.3. Установка программного обеспечения на рабочие станции осуществляется только Ответственным за ИБ или с его согласования.

9.4.4. Подключение личных устройств обучающихся и работников к ЛВС Школы запрещено без согласования с Ответственным за ИБ.

9.5. **Использование электронной почты**

9.5.1. Работники Школы используют для деловой переписки только официальный корпоративный или муниципальный адрес электронной почты.

9.5.2. Использование публичных почтовых сервисов для передачи конфиденциальной информации и персональных данных запрещено.

9.5.3. Запрещается открывать вложения и переходить по ссылкам в письмах от неизвестных отправителей (фишинг).

9.5.4. При обнаружении подозрительного письма работник обязан сообщить Ответственному за ИБ.

9.6. **Работа со съёмными носителями**

9.6.1. Съёмные носители (флеш-накопители, внешние жёсткие диски) подлежат учёту и контролю.

9.6.2. Запрещается хранить на личных носителях конфиденциальную информацию и персональные данные Школы.

9.6.3. Уничтожение съёмных носителей с конфиденциальной информацией осуществляется по акту с участием Ответственного за ИБ.

9.7. **Резервное копирование**

9.7.1. Резервное копирование данных ИС Школы осуществляется не реже одного раза в неделю.

9.7.2. Резервные копии хранятся в отдельном физическом или логическом месте, защищённом от несанкционированного доступа.

9.7.3. Периодически (не реже одного раза в квартал) проводится проверка работоспособности резервных копий.

9.8. **Управление уязвимостями и обновлениями**

9.8.1. Ответственный за ИБ регулярно проводит выявление уязвимостей в ИС Школы.

9.8.2. Критические уязвимости устраняются в срок не более 24 часов с момента обнаружения для уязвимостей на периметре сети и не более 90 дней для внутренних уязвимостей.

9.8.3. Установка обновлений программного обеспечения осуществляется только после тестирования и с разрешения Ответственного за ИБ.

9.9. **Защита обучающихся от вредоносной информации**

9.9.1. Школа обеспечивает защиту обучающихся от информации, причиняющей вред их здоровью и (или) развитию, в соответствии с Федеральным законом № 436-ФЗ.

9.9.2. Контентная фильтрация осуществляется на стороне ЕСПД: блокируются сайты, содержащие запрещённую информацию (экстремистские материалы, порнография, наркотики, суицидальный контент, азартные игры, социальные сети и др.).

9.9.3. Педагогические работники контролируют использование сети «Интернет»

обучающимися во время учебных занятий.

9.9.4. Школа проводит просветительскую работу с обучающимися и родителями по вопросам безопасного поведения в сети «Интернет».

## 10. Оценка состояния защиты информации

10.1. Оценка состояния защиты информации в Школе проводится на основе определения показателей:

10.1.1. Показателя защищённости Кзи – характеризует текущее состояние защиты информации от базового уровня угроз. Расчёт проводится не реже 1 раза в 6 месяцев в соответствии с методическими документами ФСТЭК России.

10.1.2. Показателя уровня зрелости Пзи – определяет достаточность и эффективность проводимых мероприятий по защите информации. Расчёт проводится не реже 1 раза в 2 года.

10.2. При несоответствии показателей нормированным значениям Ответственный за ИБ в течение 3 календарных дней информирует директора Школы для принятия решения о проведении мероприятий по повышению уровня защищённости.

10.3. Результаты оценки показателей Кзи и Пзи направляются в ФСТЭК России в срок не позднее 5 рабочих дней после их расчёта.

10.4. При Кзи менее 1 Школа разрабатывает план мероприятий по повышению защищённости информации.

## 11. Порядок внесения изменений в Политику

11.1. Внесение изменений и дополнений в Политику производится не реже одного раза в три года, а также при существенных изменениях:

- в законодательстве Российской Федерации в области защиты информации;
- в составе ИС и ИТИ Школы;
- по результатам оценки показателей защищённости;
- по результатам проверок контролирующих органов.

11.2. Изменения вносятся на основании приказа директора Школы.

11.3. С изменениями Политики должны быть ознакомлены все работники Школы под подпись.

## 12. Контроль за соблюдением Политики

12.1. Текущий контроль за соблюдением требований Политики возлагается на Ответственного за ИБ.

12.2. Ответственный за ИБ ежеквартально представляет директору Школы отчёт о состоянии ИБ в Школе, включающий:

- результаты мониторинга событий безопасности;
- сведения об инцидентах ИБ и принятых мерах;
- результаты контроля учётных записей и прав доступа;
- результаты проверок антивирусной защиты и обновлений ПО;
- результаты оценки показателей защищённости;
- предложения по совершенствованию системы ИБ.

12.3. Директор Школы рассматривает результаты контроля и принимает необходимые решения.

12.4. Внутренний аудит ИБ проводится не реже одного раза в год по плану, утверждённому директором Школы.