Муниципальное образовательное бюджетное учреждение
средняя общеобразовательная школа с. Мирный муниципального района
Благоварский район Республики Башкортостан

ВНУТРЕННИЕ РЕГЛАМЕНТЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Комплект внутренних регламентов по защите информации
в информационных системах образовательной организации

Утверждены приказом директора школы
от «30» сентября 2026 года № 197-ОД

с. Мирный, 2026

СОДЕРЖАНИЕ

1. Регламент управления учётными записями пользователей информационных систем
2. Регламент управления привилегированными учётными записями
3. Регламент аутентификации пользователей в информационных системах
4. Регламент предоставления и контроля удалённого доступа
5. Регламент организации доступа в Интернет через ЕСПД
6. Регламент обучения пользователей правилам информационной безопасности
7. Регламент управления уязвимостями информационных систем
8. Регламент управления обновлениями программного обеспечения
9. Регламент обработки информации ограниченного доступа
10. Регламент обеспечения физической защиты информационных систем
11. Регламент мониторинга событий информационной безопасности
12. Регламент реагирования на инциденты информационной безопасности
13. Регламент резервного копирования и восстановления данных
14. Регламент контроля уровня защищённости информации
15. Регламент работы со съёмными носителями информации
16. Регламент организации доступа подрядчиков к информационным системам

Приложения (формы журналов и таблиц учёта):

- Журнал учёта учётных записей пользователей
- Журнал учёта привилегированных учётных записей
- Матрица доступа пользователей к информационным системам
- Журнал учёта съёмных носителей информации
- Журнал инструктажей по информационной безопасности
- Журнал регистрации инцидентов информационной безопасности
- Журнал резервного копирования
- Журнал учёта обновлений программного обеспечения
- Акт уничтожения носителя информации
- Форма заявки на предоставление/изменение/отзыв доступа
- Чек-лист ежемесячной проверки состояния информационной безопасности

РЕГЛАМЕНТ № 1

Управление учётными записями пользователей информационных систем

1. Общие положения

1.1. Настоящий регламент определяет порядок создания, изменения, блокирования и удаления учётных записей пользователей информационных систем (далее – ИС), эксплуатируемых в МОБУ СОШ с. Мирный.

1.2. Регламент распространяется на все ИС, используемые в школе, включая:

- ФГИС «Моя школа» (электронный журнал/дневник);
- ФИС ОКО (Федеральная информационная система оценки качества образования);
- ФИС ФРДО (Федеральная информационная система «Федеральный реестр документов об образовании»);
- локальные ИС школы (файловые хранилища, базы данных);
- учётные записи операционных систем рабочих станций.

1.3. Ответственным за управление учётными записями назначается ответственный за информационную безопасность (далее – Администратор ИБ), назначенный приказом директора школы.

1.4. Основание для создания, изменения или удаления учётной записи – заявка по форме Приложения № 10, подписанная руководителем подразделения или директором школы.

2. Создание учётных записей

2.1. Учётная запись создаётся на основании заявки, содержащей:

- ФИО пользователя;
- должность (для сотрудников) или класс (для обучающихся);
- наименование ИС, к которой требуется доступ;
- уровень прав доступа (чтение, редактирование, администрирование);
- срок действия доступа (бессрочно / до указанной даты).

2.2. При создании учётной записи Администратор ИБ:

- присваивает уникальное имя учётной записи, исключающее анонимность доступа;
- назначает начальный пароль, соответствующий требованиям регламента № 3;
- вносит запись в журнал учёта учётных записей (приложение № 1) в течение 1 рабочего дня;
- передаёт пароль пользователю лично под подпись в журнале.

2.3. Пользователь обязан сменить пароль при первом входе в систему.

3. Изменение учётных записей

3.1. Изменение прав доступа производится на основании заявки руководителя подразделения.

3.2. При переводе сотрудника на другую должность или изменении функций Администратор ИБ в течение 2 рабочих дней актуализирует права доступа в соответствии с новыми обязанностями.

3.3. Все изменения фиксируются в Журнале учёта учётных записей с указанием даты, характера изменения и основания.

4. Блокирование учётных записей

4.1. Учётная запись блокируется в следующих случаях:

- временное отсутствие пользователя (отпуск, больничный более 30 дней, декретный отпуск) – в день получения информации от отдела кадров;
- подозрение на компрометацию учётной записи – немедленно;
- увольнение сотрудника – в последний рабочий день;
- окончание срока действия временного доступа – в указанную дату.

4.2. Блокирование производится путём изменения статуса учётной записи на «заблокирована» без удаления данных. Запись о блокировании вносится в Журнал.

5. Удаление учётных записей

5.1. Удаление учётной записи производится:

- при увольнении сотрудника – не позднее 3 рабочих дней после увольнения;
- при отчислении обучающегося – не позднее 5 рабочих дней после отчисления;
- по истечении 90 дней с момента блокирования, если доступ не был восстановлен.

5.2. Перед удалением учётной записи Администратор ИБ обеспечивает сохранение необходимых данных в соответствии с требованиями архивного хранения.

5.3. Удаление учётной записи фиксируется в Журнале с указанием даты, основание и подписи Администратора ИБ.

6. Контроль учётных записей

6.1. Администратор ИБ ежемесячно проводит проверку актуальности учётных записей:

- сверяет список активных учётных записей со списком работающих сотрудников и обучающихся;
- выявляет неиспользуемые учётные записи (нет входа более 60 дней);
- блокирует выявленные неиспользуемые учётные записи;

6.2. Результаты проверки оформляются актом, который хранится не менее 1 года.

РЕГЛАМЕНТ № 2

Управление привилегированными учётными записями

1. Общие положения

1.1. Настоящий регламент определяет порядок создания, использования, контроля и удаления привилегированных учётных записей в ИС МОБУ СОШ с. Мирный.

1.2. К привилегированным учётным записям относятся:

- учётные записи администраторов серверов и рабочих станций;
- учётные записи с правами администратора в ФГИС «Моя школа» и других внешних ИС;
- учётные записи с правами настройки сетевого оборудования;
- учётные записи управления средствами защиты информации (антивирус, межсетевой экран).

1.3. Привилегированные учётные записи создаются в минимально необходимом количестве – не более 2 на каждую ИС (основной и резервный администратор).

2. Создание и назначение

2.1. Привилегированная учётная запись создаётся на основании приказа директора школы с указанием:

- ФИО администратора;
- перечня ИС, к которым предоставляются привилегированные права;
- срок действия полномочий (не более 1 года с возможностью продления).

2.2. Запись о создании привилегированной учётной записи вносится в Журнал учёта привилегированных учётных записей (Приложение № 2).

3. Правила использования

3.1. Администратор обязан использовать привилегированную учётную запись исключительно для выполнения административных задач. Для повседневной работы (почта, просмотр сайтов, работа с документами) используется обычная учётная запись.

3.2. Запрещается:

- передавать привилегированные пароли третьим лицам;
- использовать одну привилегированную учётную запись несколькими лицами;
- оставлять сеанс привилегированного доступа без блокировки рабочего места.

3.3. Пароли привилегированных учётных записей хранятся в запечатанном конверте в сейфе у директора школы для аварийного доступа. Конверт вскрывается только в случае отсутствия администратора, о чём составляется акт.

4. Контроль

4.1. Администратор ИБ ежемесячно проверяет журнал событий привилегированного доступа и фиксирует аномальные действия.

4.2. При увольнении или смене администратора:

- все привилегированные пароли подлежат немедленной смене;
- доступ блокируется в последний рабочий день;
- учётная запись удаляется или передаётся новому администратору с обязательной сменой пароля.

РЕГЛАМЕНТ № 3
АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

1. Общие положения

1.1. Настоящий регламент устанавливает требования к аутентификации пользователей при доступе к ИС МОБУ СОШ с. Мирный.

1.2. Аутентификация пользователей осуществляется с помощью паролей. Для административных учётных записей может применяться двухфакторная аутентификация при технической возможности.

2. Требования к паролям

2.1. Пароль должен соответствовать следующим требованиям:

Параметр	Обычные пользователи	Привилегированные пользователи
Минимальная длина	не менее 8 символов	не менее 12 символов
Состав	минимум 3 из 4 групп: строчные буквы, прописные буквы, цифры, спецсимволы	все 4 группы обязательны
Срок действия	не более 90 дней	не более 60 дней
Запрет повторного использования	не менее 5 предыдущих паролей	не менее 10 предыдущих паролей
Блокировка после неудачных попыток	после 5 попыток, блокировка на 30 мин	после 3 попыток, блокировка на 60 мин

2.2. Запрещается использовать пароли, основанные на персональных данных (ФИО, дата рождения), словарных словах, последовательностях (123456, qwerty) и иной легко предсказуемой информации.

3. Хранение и передача паролей

3.1. Пароли хранятся в ИС только в виде хэш-значений. Хранение паролей в открытом виде запрещено.

3.2. Передача паролей по сети осуществляется только по защищённым протоколам (HTTPS, SSH). Запрещена передача паролей по электронной почте, в мессенджерах, СМС.

3.3. Пользователь обязан хранить пароль в тайне и не записывать его на бумажных или электронных носителях, доступных третьим лицам.

4. Смена паролей

4.1. Плановая смена паролей производится пользователем самостоятельно с учётом сроков, указанных в п. 2.1.

4.2. Внеплановая смена пароля обязательна в случаях:

- подозрение на компрометацию пароля;
- увольнение или перевод сотрудника, имевшего доступ к паролю;
- замена аппаратного или программного обеспечения, хранящего пароли;
- по требованию Администратора ИБ.

РЕГЛАМЕНТ № 4

Предоставление и контроль удалённого доступа

1. Общие положения

1.1. Настоящий регламент определяет порядок предоставления, использования и контроля удалённого доступа к информационным ресурсам МОБУ СОШ с. Мирный.

1.2. Удалённый доступ предоставляется работникам школы для выполнения служебных обязанностей вне рабочего места (дистанционное обучение, работа из дома, командировки).

2. Порядок предоставления

2.1. Удалённый доступ предоставляется на основании приказа директора школы по заявке работника (Приложение № 10).

2.2. В заявке указываются:

- ФИО работника, должность;
- цель удалённого доступа;
- перечень ИС и ресурсов, к которым требуется доступ;
- срок действия удалённого доступа;
- IP-адрес или диапазон адресов, с которых будет осуществляться доступ (при возможности).

2.3. Срок рассмотрения заявки – не более 3 рабочих дней.

3. Способы подключения

3.1. Удалённый доступ к внутренним ресурсам школы осуществляется через:

- VPN-подключение через инфраструктуру ЕСПД (при наличии технической возможности);
- веб-доступ к облачным сервисам (ФГИС «Моя школа» и др.) через защищённое соединение HTTPS.

3.2. Доступ к серверам и рабочим станциям школы из внешней сети напрямую (RDP, SSH без VPN) запрещён.

4. Правила использования

4.1. При удалённом доступе работник обязан:

- использовать только устройство, соответствующее требованиям безопасности (актуальная ОС, антивирус включён);
- не сохранять пароли в браузере и мессенджерах;
- не копировать служебную информацию на личные устройства без разрешения;
- завершать сеанс удалённого доступа после окончания работы.

4.2. Запрещено передавать учётные данные и параметры VPN-подключения третьим лицам.

5. Контроль

5.1. Администратор ИБ ведёт журнал удалённых подключений с фиксацией:

- ФИО пользователя, даты и времени подключения/отключения;

- IP-адреса, с которого осуществлено подключение;
- доступных ресурсов.

5.2. Проверка журналов удалённого доступа производится ежемесячно.

5.3. При выявлении несанкционированных подключений доступ блокируется немедленно, проводится расследование в соответствии с Регламентом № 12.

РЕГЛАМЕНТ № 5

Организация доступа в интернет через ЕСПД

1. Общие положения

1.1. Настоящий регламент определяет порядок организации, использования и контроля доступа в Интернет для работников и обучающихся МОБУ СОШ с. Мирный.

1.2. Доступ в Интернет в школе организован через Единую сеть передачи данных (ЕСПД) Республики Башкортостан. ЕСПД обеспечивает:

- Подключение школы к сети Интернет через защищённый канал;
- Контентную фильтрацию на уровне провайдера ЕСПД;
- Маршрутизацию и адресацию внутренних узлов школы.

1.3. Доступ в Интернет предоставляется только через сетевое оборудование и каналы связи ЕСПД. Использование альтернативных каналов (мобильные модемы, Wi-Fi-роутеры с прямым выходом в Интернет, не подключённые к ЕСПД) для рабочих станций, обрабатывающих служебную информацию, запрещено.

2. Категории пользователей и режимы доступа

2.1. Доступ в Интернет разделён по категориям пользователей:

Категория	Режим доступа	Ограничения
Работники (педагоги, администрация)	Полный доступ через ЕСПД с контентной фильтрацией	Запрет доступа к ресурсам, не связанным с исполнением служебных обязанностей
Обучающиеся	Доступ под руководством педагога	Доступ только к образовательным ресурсам; сайты с деструктивным контентом блокируются фильтром ЕСПД
Администратор ИБ	Полный доступ для управления настройками	Доступ к панели управления фильтрацией (при наличии)

3. Контентная фильтрация

3.1. Контентная фильтрация осуществляется на уровне ЕСПД. Дополнительно в школе может применяться локальная фильтрация средствами операционной системы или антивирусного ПО.

3.2. Категории ресурсов, доступ к которым блокируется:

- ресурсы с противоправным контентом (экстремизм, наркотики, оружие);
- порнографические и иные ресурсы, несовместимые с образовательной средой;
- социальные сети в учебное время (по решению администрации школы);
- файловые обменники и торренты (за исключением образовательных нужд).

3.3. Педагог, обнаруживший, что образовательный ресурс ошибочно заблокирован фильтром ЕСПД, подаёт заявку Администратору ИБ для обращения в службу технической поддержки ЕСПД с просьбой разблокировать ресурс.

3.4. При обнаружении попытки обхода контентной фильтрации обучающимся педагог обязан пресечь попытку и сообщить директору школы.

4. Использование ресурсов Интернета

4.1. Работники школы имеют право использовать Интернет для:

- Подготовки к учебным занятиям и методической работы;

- Работы с государственными информационными системами (ФГИС «Моя школа», ФИС ОКО, ФИС ФРДО и др.);
- Профессионального развития (вебинары, курсы повышения квалификации);
- Коммуникации с родителями и образовательными организациями.

4.2. Обучающиеся используют Интернет только в учебных целях под контролем педагога.

4.3. Запрещается:

- Скачивать и устанавливать ПО из непроверенных источников;
- Открывать вложения из подозрительных писем (фишинг);
- Передавать персональные данные на неконтролируемые сайты;
- Использовать Интернет для коммерческой деятельности.

5. Контроль и журналирование

5.1. Журналирование доступа в Интернет осуществляется средствами ЕСПД. Дополнительно Администратор ИБ может вести журнал доступа на уровне школьного шлюза.

5.2. Анализ журналов доступа производится ежемесячно на предмет:

- попыток доступа к заблокированным ресурсам;
- аномального трафика (большие объёмы скачивания);
- доступа в неурочное время.

5.3. При выявлении нарушений доступ конкретного пользователя может быть ограничен по решению директора школы.

РЕГЛАМЕНТ № 6

Обучение пользователей правилам информационной безопасности

1. Общие положения

1.1. Настоящий регламент определяет порядок обучения работников и обучающихся МОБУ СОШ с. Мирный правилам информационной безопасности.

1.2. Обучение направлено на формирование у пользователей навыков безопасной работы с информацией, предотвращение инцидентов и снижение рисков, связанных с действиями человека.

2. Виды обучения

2.1. Обучение подразделяется на следующие виды:

Вид	**Периодичность**	**Категория**	**Ответственный**
Вводный инструктаж	При приёме на работу / начале учебного года	Работники / обучающиеся	Администратор ИБ / классный руководитель
Периодический инструктаж	Не реже 1 раза в полгода	Работники	Администратор ИБ
Внеплановый инструктаж	При возникновении инцидента ИБ, обновлении регламентов	Работники	Администратор ИБ
Тренировка по реагированию на инциденты	Не реже 1 раза в год	Администратор ИБ, ответственные лица	Директор школы

3. Содержание обучения

3.1. Программа обучения для работников включает:

- требования законодательства в области защиты информации и персональных данных;
- правила работы с паролями и учётными записями;
- правила безопасной работы в Интернете, защита от фишинга;
- порядок работы со съёмными носителями;
- действия при обнаружении подозрительных файлов, писем, устройств;
- порядок реагирования на инциденты ИБ;
- правила работы с персональными данными обучающихся.

3.2. Программа обучения для обучающихся включает:

- правила безопасного поведения в Интернете;
- защита от интернет-мошенничества и фишинга;
- недопустимость распространения персональных данных в социальных сетях;
- ответственность за неправомерный доступ к информации.

4. Регистрация обучения

4.1. Все инструктажи регистрируются в Журнале инструктажей по информационной безопасности (Приложение № 5).

4.2. Работники расписываются в журнале за прохождение инструктажа.

4.3. Для обучающихся регистрация проводится классным руководителем в классном журнале отдельной графой.

5. Проверка знаний

5.1. После периодического инструктажа проводится проверка знаний в форме тестирования (бумажного или электронного).

5.2. Работник, не прошедший проверку знаний, повторно проходит инструктаж в течение 10 рабочих дней. При повторном непрохождении – доклад директору школы.

РЕГЛАМЕНТ № 7

Управление уязвимостями информационных систем

1. Общие положения

1.1. Настоящий регламент определяет порядок выявления, оценки, устранения и контроля уязвимостей в ИС МОБУ СОШ с. Мирный.

1.2. Под уязвимостью понимается недостаток или ошибка в программном обеспечении, конфигурации или архитектуре ИС, которая может быть использована для нарушения безопасности информации.

2. Выявление уязвимостей

2.1. Источниками информации об уязвимостях являются:

- уведомления производителей ПО и операционных систем;
- информационные сообщения ФСТЭК России, ФСБ России, Роскомнадзора;
- результаты антивирусного сканирования;
- результаты внутренних проверок и аудитов;
- сообщения пользователей о необычном поведении систем.

2.2. Администратор ИБ регулярно (не реже 1 раза в месяц) проверяет актуальные уведомления об уязвимостях ПО, используемого в школе.

3. Оценка уязвимостей

3.1. Каждая выявленная уязвимость оценивается по уровню критичности:

Уровень	Описание	Срок устранения
Критический	Возможность удалённого выполнения кода, полного доступа к системе, утечки персональных данных	Не более 24 часов
Высокий	Возможность несанкционированного доступа, нарушения целостности данных	Не более 72 часов
Средний	Возможность получения информации о системе, нарушения доступности отдельных сервисов	Не более 7 дней
Низкий	Ограниченное воздействие, сложность эксплуатации	Не более 30 дней

4. Устранение уязвимостей

4.1. Устранение уязвимости производится путём:

- установки обновлений и патчей от производителя ПО;
- изменения конфигурации системы;
- отключения уязвимых компонентов (если обновление невозможно);
- применения компенсирующих мер (дополнительные правила межсетевого экрана, ограничение доступа).

4.2. Если уязвимость невозможно устранить в установленный срок, Администратор ИБ применяет компенсирующие меры и уведомляет директора школы.

4.3. Все выявленные уязвимости и работы по их устранению фиксируются в журнале, который ведёт Администратор ИБ.

РЕГЛАМЕНТ № 8

Управление обновлениями программного обеспечения

1. Общие положения

1.1. Настоящий регламент определяет порядок установки, тестирования и контроля обновлений программного обеспечения в ИС МОБУ СОШ с. Мирный.

1.2. Обновлению подлежат: операционные системы, прикладное ПО, антивирусное ПО, средства защиты информации, прошивки сетевого оборудования.

2. Источники обновлений

2.1. Обновления загружаются только из официальных источников:

- Центр обновления Windows / Microsoft Update;
- официальные сайты производителей ПО;
- серверы управления антивирусной защитой;
- Центр управления ЕСПД (для обновлений сетевого оборудования, если применимо).

2.2. Загрузка обновлений из сторонних источников, торрентов и файловых обменников запрещена.

3. Порядок установки обновлений

3.1. Перед установкой обновлений на рабочих станциях Администратор ИБ:

- проверяет наличие обновлений на тестовой станции (при наличии);
- создаёт точку восстановления или резервную копию системы;
- согласовывает время установки с пользователем (вне учебного процесса).

3.2. Установка критических обновлений безопасности производится в течение 24 часов с момента их публикации. Установка функциональных обновлений – в течение 30 дней.

3.3. Для серверов обновления устанавливаются только после тестирования и в заранее запланированное технологическое окно (выходные дни, ночное время).

4. Контроль и журналирование

4.1. Администратор ИБ ведёт Журнал учёта обновлений (Приложение № 8), в котором фиксирует:

- дату установки, наименование ПО, версию обновления, перечень исправленных уязвимостей;
- перечень обновлённых рабочих станций/серверов;
- результат установки (успешно / ошибка).

4.2. Ежемесячно Администратор ИБ проводит проверку актуальности установленного ПО на всех рабочих станциях школы.

РЕГЛАМЕНТ № 9
Обработка информации ограниченного доступа

1. Общие положения

1.1. Настоящий регламент определяет порядок обработки, хранения, передачи и уничтожения информации ограниченного доступа в МОБУ СОШ с. Мирный.

1.2. К информации ограниченного доступа в школе относятся:

- персональные данные обучающихся, их родителей (законных представителей) и работников (ФЗ № 152 «О персональных данных»);
- служебная информация, доступ к которой ограничен в соответствии с законодательством (например, сведения, составляющие тайну);
- учётные данные и пароли доступа к ИС;
- конфигурационная информация средств защиты информации.

1.3. Обработка персональных данных в школе осуществляется в соответствии с Политикой обработки персональных данных, утверждаемой отдельно.

2. Сбор и обработка

2.1. Сбор персональных данных осуществляется только на законных основаниях с письменного согласия субъекта или его законного представителя.

2.2. Обработка персональных данных ограничивается конкретными, заранее определёнными и законными целями:

- организация образовательного процесса;
- ведение учёта обучающихся;
- оформление документов об образовании;
- обеспечение безопасности обучающихся.

2.3. Запрещается использовать персональные данные в целях, не связанных с образовательной деятельностью школы.

3. Хранение

3.1. Персональные данные хранятся:

- В электронном виде — в ИС школы и государственных ИС (ФГИС «Моя школа» и др.);
- На бумажных носителях — в запираемых шкафах или сейфах в специально отведённых помещениях.

3.2. Доступ к помещениям, где хранятся носители с персональными данными, ограничен. Ключи хранятся у ответственного лица.

3.3. Срок хранения персональных данных определяется в соответствии с законодательством и номенклатурой дел школы.

4. Передача

4.1. Передача персональных данных третьим лицам осуществляется только на законных основаниях (запросы уполномоченных органов, согласие субъекта).

4.2. Передача электронных персональных данных по сети осуществляется только по

защищённым каналам (HTTPS, через ЕСПД). Запрещена передача по открытой электронной почте без шифрования.

4.3. Передача данных на съёмных носителях осуществляется с учётом требований Регламента № 15.

5. Уничтожение

5.1. Уничтожение носителей с информацией ограниченного доступа производится в соответствии с Регламентом № 15.

5.2. Уничтожение электронных данных производится путём гарантированного удаления (перезапись, форматирование с уничтожением данных) с составлением акта.

5.3. Бумажные носители уничтожаются путём shredder-обработки (шредер) с составлением акта уничтожения (Приложение № 9).

РЕГЛАМЕНТ № 10

Обеспечение физической защиты информационных систем

1. Общие положения

1.1. Настоящий регламент определяет требования к физической защите помещений, оборудования и носителей информации в МОБУ СОШ с. Мирный.

1.2. Физическая защита направлена на предотвращение:

- Несанкционированного доступа в помещения с ИС и носителями информации;
- Хищения или порчи оборудования и носителей;
- Нарушения работы ИС вследствие физических воздействий (пожар, затопление, отключение питания).

2. Защита рабочих станций

2.1. Рабочие станции, обрабатывающие информацию ограниченного доступа, расположены в кабинетах с ограниченным доступом в нерабочее время (закрываются на ключ).

2.2. В кабинетах информатики доступ обучающихся к системному блоку ограничен: порты USB могут быть заблокированы программно, системный блок размещён в недоступном для обучающихся месте.

2.3. Оборудование, хранящее информацию ограниченного доступа, по возможности закрепляется (стопоры, замки корпуса).

3. Защита сетевого оборудования

3.1. Сетевое оборудование (коммутаторы, маршрутизаторы, оборудование ЕСПД) размещается в местах с ограниченным физическим доступом (серверное помещение, запираемые шкафы).

3.2. Кабельная инфраструктура проложена с учётом минимизации риска случайного повреждения. Концы кабелей маркированы.

4. Контроль физического доступа

4.1. Ключи от помещений с ИС хранятся у ответственных лиц и сдаются по журналу.

4.2. В нерабочее время, выходные и праздничные дни помещения с ИС опечатываются.

4.3. При обнаружении нарушения целостности пломб (печатей) или признаков несанкционированного доступа ответственный работник немедленно сообщает директору школы и Администратору ИБ для расследования.

РЕГЛАМЕНТ № 11
Мониторинг событий информационной безопасности

1. Общие положения

1.1. Настоящий регламент определяет перечень регистрируемых событий ИБ, порядок сбора, хранения и анализа журналов событий в ИС МОБУ СОШ с. Мирный.

1.2. Цель мониторинга – своевременное выявление инцидентов ИБ, расследование их причин и предотвращение повторения.

2. Регистрируемые события

2.1. В ИС школы регистрируются следующие события ИБ:

Событие	Источник	Срок хранения
Вход/выход пользователей в ИС	Журналы ОС, ФГИС «Моя школа»	Не менее 90 дней
Неудачные попытки аутентификации	Журналы ОС, ИС	Не менее 90 дней
Блокировка учётной записи	Журналы ОС, ИС	Не менее 1 года
Изменение прав доступа	Журналы ИС	Не менее 1 года
Создание/удаление учётной записи	Журналы ИС	Не менее 1 года
Установка/удаление ПО	Журналы ОС	Не менее 1 года
Срабатывание антивируса	Журнал антивирусного ПО	Не менее 1 года
Подключение съёмных носителей	Журналы ОС (при возможности)	Не менее 90 дней
Удалённые подключения (VPN)	Журнал VPN/ЕСПД	Не менее 90 дней
Доступ в Интернет (через ЕСПД)	Журналы ЕСПД	Согласно политике ЕСПД

3. Порядок сбора и анализа

3.1. Администратор ИБ ежемесячно анализирует журналы событий на предмет:

- аномального количества неудачных попыток входа (возможный подбор пароля);
- входа в нерабочее время;
- изменений конфигурации, не оформленных документально;
- срабатывания антивирусной защиты;
- подключений неразрешённых съёмных носителей.

3.2. По результатам анализа составляется отчёт, который представляется директору школы ежеквартально.

3.3. При выявлении подозрительной активности немедленно инициируется процедура реагирования в соответствии с Регламентом № 12.

4. Защита журналов

4.1. Доступ к журналам событий ограничен. Право просмотра предоставлено Администратору ИБ и директору школы.

4.2. Журналы защищены от несанкционированного изменения. Запрещено удаление или изменение записей журналов без документального оформления причины.

РЕГЛАМЕНТ № 12

Реагирование на инциденты информационной безопасности

1. Общие положения

1.1. Настоящий регламент определяет порядок обнаружения, регистрации, расследования и устранения инцидентов ИБ в МОБУ СОШ с. Мирный.

1.2. Инцидент ИБ – событие, указывающее на нарушение или угрозу нарушения безопасности информации (несанкционированный доступ, утечка данных, заражение вредоносным ПО, сбой системы и т. д.).

2. Классификация инцидентов

Уровень	Описание	Примеры
Критический	Угроза жизни, утечка персональных данных массового характера, полная остановка ИС	Взлом сервера, массовая утечка ПДн обучающихся, уничтожение базы данных
Высокий	Серьёзное нарушение безопасности, затрагивающее часть ИС	Заражение рабочей станции вирусом-шифровальщиком, несанкционированный доступ к журналу
Средний	Нарушение, ограниченное по масштабу	Подбор пароля к одной учётной записи, фишинговое письмо открыто пользователем
Низкий	Незначительное нарушение или попытка	Попытка доступа к заблокированному сайту, неудачная попытка подключения флешки

3. Обнаружение и регистрация

3.1. Любой пользователь, обнаруживший подозрительное событие или инцидент, обязан немедленно сообщить Администратору ИБ устно, а затем в течение 1 рабочего дня – письменно (заявка, электронное письмо).

3.2. Администратор ИБ регистрирует инцидент в Журнале регистрации инцидентов ИБ (Приложение № 6) с указанием:

- дата и время обнаружения;
- описание инцидента и его уровня;
- источник информации об инциденте;
- принятые первоочередные меры.

4. Первоочередные действия

4.1. При обнаружении инцидента Администратор ИБ немедленно принимает меры по локализации:

- критический/высокий уровень — отключить затронутую систему от сети, заблокировать учётные записи, сохранить доказательства (снимки экрана, копии журналов);
- средний уровень — ограничить доступ к затронутым ресурсам, провести анализ;
- низкий уровень — зафиксировать событие, провести мониторинг.

4.2. О инцидентах критического и высокого уровня Администратор ИБ немедленно уведомляет директора школы.

4.3. При инцидентах, связанных с утечкой персональных данных, директор школы в установленном законодательством порядке уведомляет Роскомнадзор (в течение 72 часов с момента обнаружения).

5. Расследование

5.1. Расследование инцидента проводится комиссией, назначаемой приказом директора школы, в составе не менее 3 человек.

5.2. Комиссия:

- устанавливает причину инцидента и объём ущерба;
- определяет нарушителя (при наличии);
- разрабатывает рекомендации по предотвращению подобных инцидентов.

5.3. Срок расследования – не более 10 рабочих дней. По результатам составляется акт, который утверждается директором школы.

6. Устранение последствий

6.1. После локализации инцидента Администратор ИБ:

- восстанавливает работоспособность ИС из резервных копий (при необходимости);
- меняет скомпрометированные пароли;
- устраняет уязвимости, использованные для атаки;
- проверяет систему на наличие скрытых угроз (дополнительное антивирусное сканирование).

6.2. Рекомендации комиссии внедряются в срок, указанный в акте расследования, но не более 30 дней.

РЕГЛАМЕНТ № 13

Резервное копирование и восстановление данных

1. Общие положения

1.1. Настоящий регламент определяет порядок создания, хранения и использования резервных копий данных в ИС МОБУ СОШ с. Мирный.

1.2. Цель резервного копирования – обеспечение возможности восстановления данных в случае их утраты, повреждения или уничтожения.

2. Объекты резервного копирования

2.1. Резервному копированию подлежат:

Объект	Периодичность	Тип копии	Срок хранения
База данных электронного журнала (ФГИС «Моя школа» — локальные данные)	Ежедневно	Инкрементальная	30 дней
Файловые хранилища школы (документы, методические материалы)	Еженедельно	Полная	90 дней
Конфигурации серверов и сетевого оборудования	При изменении	Полная	180 дней
Системные разделы серверов	Ежемесячно	Образ диска	90 дней
Базы данных с персональными данными (локальные)	Ежедневно	Полная + инкрементальная	Не менее 1 года

3. Хранение резервных копий

3.1. Резервные копии хранятся:

- Основная копия – на отдельном носителе (внешний жёсткий диск, сетевое хранилище), не подключённом к рабочей сети постоянно;
- Дополнительная копия – в отдельном помещении (кабинет директора или сейф), защищённом от несанкционированного доступа.

3.2. Запрещается хранить резервные копии на том же физическом устройстве, что и оригинальные данные.

3.3. Носители с резервными копиями маркируются и учитываются в Журнале резервного копирования (Приложение № 7).

4. Восстановление данных

4.1. Восстановление данных из резервной копии производится на основании заявки, утверждённой директором школы.

4.2. Перед восстановлением Администратор ИБ:

- проверяет целостность резервной копии;
- создает копию текущего состояния системы (для возможного отката);
- восстанавливает данные и проверяет их работоспособность.

4.3. Проверка работоспособности резервных копий (тестовое восстановление) проводится не реже 1 раза в квартал.

РЕГЛАМЕНТ № 14

Контроль уровня защищённости информации

1. Общие положения

1.1. Настоящий регламент определяет порядок проведения внутреннего контроля и аудита состояния информационной безопасности в МОБУ СОШ с. Мирный.

1.2. Цель контроля — оценка соответствия принимаемых мер защиты информации требованиям законодательства и внутренним документам школы, выявление недостатков и их устранение.

2. Виды контроля

2.1. Внутренний контроль ИБ включает:

Вид контроля	Периодичность	Ответственный
Ежемесячная проверка состояния ИБ	Ежемесячно	Администратор ИБ
Ежеквартальный аудит	Ежеквартально	Администратор ИБ + комиссия
Годовой аудит ИБ	Ежегодно	Комиссия, назначенная директором
Внеплановая проверка	При инциденте, по требованию директора	Администратор ИБ

3. Содержание ежемесячной проверки

3.1. Ежемесячная проверка проводится по чек-листу (Приложение № 11) и включает контроль:

- актуальности учётных записей (нет ли неактивных, заблокированных);
- своевременности установки обновлений ОС и ПО;
- работоспособности антивирусной защиты (актуальность баз, статус защиты);
- наличия и целостности резервных копий;
- соблюдения правил физической защиты (закрытие помещений, опечатывание);
- отсутствия неразрешённых подключений к сети;
- актуальности матрицы доступа.

4. Содержание ежеквартального и годового аудита

4.1. Ежеквартальный аудит дополнительно включает:

- анализ журналов событий за квартал;
- проверку выполнения рекомендаций предыдущих аудитов;
- оценку уровня осведомлённости пользователей (опрос/тестирование).

4.2. Годовой аудит включает:

- полную проверку всех элементов системы защиты информации;
- оценку соответствия требованиям ФЗ № 152, приказам ФСТЭК и ФСБ;
- пересмотр актуальности внутренних регламентов и инструкций;
- формирование плана мероприятий по повышению уровня ИБ на следующий год.

5. Оформление результатов

5.1. Результаты каждой проверки оформляются актом, который подписывается Администратором ИБ и утверждается директором школы.

5.2. В акте указываются:

- выявленные нарушения и недостатки;
- сроки устранения;
- ответственные за устранение;
- рекомендации по улучшению.

5.3. Контроль устранения выявленных нарушений ведётся Администратором ИБ. Отчёт об устранении представляется директору в установленный срок.

РЕГЛАМЕНТ № 15

Работа со съёмными носителями информации

1. Общие положения

1.1. Настоящий регламент определяет порядок учёта, использования, проверки и уничтожения съёмных носителей информации в МОБУ СОШ с. Мирный.

1.2. К съёмным носителям относятся: USB-флеш-накопители, внешние жёсткие диски, CD/DVD-диски, SD-карты и иные портативные устройства хранения данных.

2. Учёт съёмных носителей

2.1. Все съёмные носители, используемые для работы с информацией ограниченного доступа, подлежат обязательному учёту в Журнале учёта съёмных носителей (Приложение № 4).

2.2. Учётные записи носителей включают:

- инвентарный номер;
- тип и объём носителя;
- дату постановки на учёт;
- ответственное лицо;
- цель использования;
- дату снятия с учёта (при списании).

2.3. Носители маркируются (наклейка с инвентарным номером).

3. Правила использования

3.1. Перед подключением съёмного носителя к рабочей станции обязательно:

- проверка носителя антивирусным ПО с актуальными базами;
- сканирование на наличие вредоносных программ.

3.2. Запрещается:

- подключать личные съёмные носители к рабочим станциям, обрабатывающим информацию ограниченного доступа;
- подключать неразрешённые съёмные носители в кабинете информатики обучающимися без разрешения педагога;
- выносить учётные съёмные носители за пределы школы без разрешения директора;
- хранить на съёмных носителях нешифрованные персональные данные (при технической возможности шифрования).

3.3. На рабочих станциях, обрабатывающих информацию ограниченного доступа, порты USB могут быть программно заблокированы. Разрешение на подключение выдаёт Администратор ИБ.

4. Уничтожение носителей

4.1. Уничтожение съёмных носителей, содержащих информацию ограниченного доступа, производится в следующих случаях:

- носитель вышел из строя и не подлежит ремонту;
- информация на носителе больше не нужна и подлежит уничтожению;

- окончен срок эксплуатации носителя.

4.2. Уничтожение производится путём физического уничтожения (разрушение корпуса, размагничивание, резка, сжигание) с составлением Акта уничтожения (Приложение № 9).

4.3. Акт подписывается комиссией из не менее 3 человек (Администратор ИБ, представитель администрации, представитель коллектива).

РЕГЛАМЕНТ № 16

Организация доступа подрядчиков к информационным системам

1. Общие положения

1.1. Настоящий регламент определяет порядок предоставления и контроля доступа к ИС МОБУ СОШ с. Мирный сторонним организациям и подрядчикам (обслуживание оборудования, техническая поддержка ЕСПД, обслуживание ПО).

1.2. Подрядчики — представители сторонних организаций, привлекаемые для установки, настройки, ремонта или обслуживания оборудования и ПО школы.

2. Условия предоставления доступа

2.1. Доступ подрядчиков к ИС предоставляется на основании:

- Договора на оказание услуг, предусматривающего обязательства по сохранению конфиденциальности;
- Приказа директора школы о допуске подрядчика с указанием перечня работ, срока и ответственного от школы.

2.2. До начала работ подрядчик:

- Знакомится с правилами ИБ школы под подпись;
- Подписывает обязательство о неразглашении информации ограниченного доступа.

2.3. Удалённый доступ подрядчиков (при необходимости) предоставляется в соответствии с Регламентом № 4 и только на время проведения работ.

3. Правила проведения работ

3.1. Работы подрядчика в помещениях с ИС проводятся:

- В присутствии Администратора ИБ или назначенного работника школы;
- Вне учебного процесса (при возможности);
- С записью в журнале посещений серверного помещения.

3.2. Подрядчику запрещено:

- Самостоятельно копировать данные из ИС школы на свои носители;
- Изменять настройки средств защиты информации без согласования с Администратором ИБ;
- Подключать к сети школы оборудование, не согласованное с Администратором ИБ.

3.3. При проведении работ, связанных с доступом к персональным данным, используется временное предоставление прав с немедленным отзывом по завершении работ.

4. Контроль и завершение работ

4.1. По завершении работ Администратор ИБ:

- Проверяет целостность настроек ИС и средств защиты;
- Блокирует и удаляет временные учётные записи подрядчика;
- Меняет пароли, если подрядчик имел к ним доступ;
- Составляет акт приёмки работ с указанием изменений, внесённых в ИС.

4.2. При обнаружении несанкционированных действий подрядчика — немедленно блокируется доступ и сообщается директору школы для принятия мер в соответствии с условиями договора.

Приложения

Приложение № 1

Журнал учёта учётных записей пользователей

Форма журнала (заполняется Администратором ИБ):

№	Дата	ФИО пользователя	Должность/класс	Наименование ИС	Имя уч. записи	Уровень прав	Дата создания	Дата блокировки	Дата удаления	Основание	Подпись ИБ
1											
2											
3											

Приложение № 2

Журнал учёта привилегированных учётных записей

№	Дата создания	ФИО администратора	ИС / ресурс	Имя уч. записи	Основание (приказ)	Срок действия	Дата блокировки	Дата удаления	Подпись директора	Подпись ИБ
1										
2										
3										

Приложение № 3

Матрица доступа пользователей к информационным системам

Должность	ФГИС «Моя школа»	ФИС ОКО	ФИС ФРДО	Локальная сеть	Почта	Интернет (ЕСПД)
Директор	Чтение/ред.	Чтение/ред.	Чтение/ред.	Чтение	Чтение/ред.	Полный
Зам. по УВР	Чтение/ред.	Чтение/ред.	—	Чтение	Чтение/ред.	Полный
Учитель	Чтение/ред.	Чтение	—	Чтение	Чтение/ред.	Полный
Секретарь	Чтение	—	Чтение/ред.	Чтение/ред.	Чтение/ред.	Полный
Админ. ИБ	Админ.	Админ.	Админ.	Админ.	Админ.	Полный
Обучающийся	Чтение	—	—	—	—	Фильтр.

Приложение № 4

Журнал учёта съёмных носителей информации

№	Инв. №	Тип носителя	Объём	Дата постановки на учёт	Ответственный	Цель использования	Дата снятия с учёта	Основание	Подпись ИБ
1									
2									
3									

Приложение № 5

Журнал инструктажей по информационной безопасности

№	Дата	Вид инструктажа	ФИО инструктируемого	Должность/класс	Тема	Подпись инструктируемого	Подпись инструктирующего
1							
2							

Приложение № 6

Журнал регистрации инцидентов информационной безопасности

№	Дата/время обнаружения	Описание инцидента	Уровень	Источник информации	Первые меры	Дата расследования	Результат/рекомендации	Подпись ИБ
1								
2								

Приложение № 7

Журнал резервного копирования

№	Дата	Объект копирования	Тип копии (полная/инкр.)	Носитель (инв. №)	Объём	Результат (успешно/ошибка)	Подпись ИБ
1							
2							

Приложение № 8

Журнал учёта обновлений программного обеспечения

№	Дата	Наименование ПО	Версия обновления	Тип (безопасность/функцион.)	Рабочие станции/серверы	Результат	Подпись ИБ
1							
2							

Приложение № 9

Акт уничтожения носителя информации

Комиссия, назначенная приказом директора МОБУ СОШ с. Мирный от «___» _____ 20___ г. № ___

В составе:

- Председатель: _____ (_____)
- Член комиссии: _____ (_____)
- Член комиссии: _____ (_____)

На основании приказа произвела уничтожение следующего носителя информации:

№	Инв. №	Тип носителя	Объём	Содержание информации	Способ уничтожения	Дата уничтожения
1						

Носитель уничтожен полностью, восстановление информации невозможно.

Подписи членов комиссии:

Председатель: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/

Приложение № 10
Форма заявки на предоставление / изменение / отзыв доступа

Директору МОБУ СОШ с. Мирный
от _____
должность: _____

ЗАЯВКА

Прошу предоставить / изменить / отозвать (нужное подчеркнуть) доступ:

Параметр	Значение
ФИО пользователя	
Должность / класс	
Наименование ИС	
Запрашиваемые права	
Тип заявки (создание/изменение/блокировка/удаление)	
Срок действия	
Основание	

Подпись заявителя: _____ Дата: _____

Согласовано:
Администратор ИБ: _____ Дата: _____
Директор школы: _____ Дата: _____

Приложение № 11

Чек-лист ежемесячной проверки состояния информационной безопасности

Месяц: _____ Год: _____ Проверяющий: _____

№ п/п	Пункт проверки	Результат (да/нет)	Примечание
1	Актуальность учётных записей (нет неактивных, заблокированных)		
2	Своевременность установки обновлений ОС и ПО		
3	Антивирусные базы актуальны на всех рабочих станциях		
4	Антивирус включён и работает на всех станциях		
5	Резервные копии созданы и проверены		
6	Носители резервных копий хранятся в надлежащих условиях		
7	Помещения с ИС закрываются в нерабочее время		
8	Серверное помещение опечатано, пломбы целы		
9	Журналы событий проверены, аномалии не выявлены		
10	Матрица доступа актуальна		
11	Съёмные носители учтены, маркированы		
12	Журналы ИБ заполнены и актуальны		
13	Нет неразрешённых подключений к сети		
14	Контентная фильтрация через ЕСПД работает		

Выявленные нарушения:

Меры по устранению и сроки:

Подпись проверяющего: _____ Дата: _____