Приложение 1
к приказу МАОУ «Школа № 5 им. И.О. Родобольского»
от 09.01.2025г. № 2/3-о/д

ПОРЯДОК
осуществления информационной безопасности, обеспечивающих защиту от несанкционированного доступа к информационным ресурсам МАОУ «Школа № 5 им. И.О. Родобольского»

1. Общие положения

1.1.Настоящий Порядок разработан в соответствии с требованиями:
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
- Приказа Минкомсвязи России от 16.06.2014 № 161 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящий Порядок определяет организационные и технические меры по защите информационных ресурсов от несанкционированного доступа (НСД) в МАОУ «Школа № 5 им. И.О. Родобольского».

1.3. Действие Порядка распространяется на:
- Педагогических работников
- Административный персонал
- Обучающихся
- Технический персонал
- Сторонних лиц, осуществляющих деятельность в организации

1.4. Информационные ресурсы, подлежащие защите:
- Официальный сайт образовательной организации
- Система «Электронный дневник/журнал»
- Базы персональных данных.
- Библиотечные информационные ресурсы.

2. Организационные меры защиты

2.1. Разграничение прав доступа:
- Создание отдельных групп пользователей с дифференцированными правами доступа.
- Регулярный аудит учетных записей (не реже 1 раза в четверть).
- Немедленная блокировка учетных записей уволенных сотрудников и выпускников.

2.2. Управление учетными записями:
- Обязательная идентификация и аутентификация пользователей.
- Использование сложных паролей (не менее 8 символов, с использованием различных групп символов).
- Смена паролей не реже 1 раза в 90 дней.

2.3. Контроль физического доступа:
- Ограничение доступа в компьютерные классы вне учебного времени.
- Видео наблюдение в местах размещения критически важного оборудования.

2.4. Регламентация работ:
- Запрет на установку нелицензионного программного обеспечения.
- Ограничение доступа к ресурсам, не связанным с образовательным процессом.
- Регламент использования персональных устройств в сети организации.

3. Технические меры защиты
3.1. Защита сетевой инфраструктуры:
- Межсетевые экраны и система фильтрации трафика
- Система обнаружения и предотвращения вторжений (IDS/IPS)
- Средства антивирусной защиты

3.2. Защита каналов связи:
- Шифрование передаваемой информации при работе с персональными данными
- Защита беспроводных сетей

3.3. Мониторинг и аудит:
- Периодическое тестирование системы защиты

4. Действия при инцидентах НСД
4.1. Немедленное информирование системного администратора и руководителя организации
4.2. Сохранение доказательственной базы

4.3. Информирование уполномоченного органа по защите прав субъектов персональных данных (при утечке персональных данных)
4.4. Проведение служебного расследования

5. Обязанности и ответственность
5.1. Ответственный за информационную безопасность:
- Внедрение и поддержание мер защиты
- Проведение инструктажей пользователей
- Реагирование на инциденты информационной безопасности

5.2. Пользователи обязаны:
- Соблюдать правила использования информационных ресурсов
- Немедленно сообщать о подозрительных действиях в системе
- Не передавать учетные данные третьим лицам

5.3. Администрация организации:
- Обеспечение необходимых ресурсов для защиты информации
- Контроль соблюдения настоящего Порядка

6. Заключительные положения
6.1. Настоящий Порядок вступает в силу со дня издания приказа об утверждении и действует до замены новым документом.
6.2. Все пользователи должны быть ознакомлены с Порядком под подпись при приеме на работу/зачислении в организацию.

ПРИЛОЖЕНИЕ 1

к Порядку осуществления информационной безопасности
МАОУ «Школа № 5 им. И.О. Родобольского»

ПЕРЕЧЕНЬ ЗАЩИЩАЕМЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ

№ п/п	Наименование информационного ресурса	Категория защищаемой информации	Уровень защищенности	Ответственный
1	Официальный сайт образовательной организации	Открытая информация, персональные данные	Средний	Ответственный за сайт
2	Система «Электронный дневник/журнал»	Персональные данные, образовательные результаты	Высокий	Системный администратор
3	Базы персональных данных обучающихся и сотрудников	Персональные данные, специальные категории данных	Высокий	Ответственный за персональные данные
4	Архивы образовательных программ	Интеллектуальная собственность, методические материалы	Средний	Заместитель директора по УВР
5	Библиотечные информационные ресурсы	Библиотечный фонд, электронные ресурсы	Базовый	Заведующий библиотекой
6	Система видео наблюдения	Данные видео наблюдения	Средний	Ответственный за безопасность
7	Корпоративная электронная почта	Деловая переписка, персональные данные	Средний	Системный администратор

ПРИЛОЖЕНИЕ 2
к Порядку осуществления информационной безопасности
МАОУ «Школа № 5 им. И.О. Родобольского»

ИНСТРУКЦИЯ ПО СОЗДАНИЮ И ХРАНЕНИЮ ПАРОЛЕЙ

1. Требования к созданию паролей:
- Минимальная длина: 8 символов
- Обязательное использование символов разных групп:
  - Прописные латинские буквы (A-Z)
  - Строчные латинские буквы (a-z)
  - Цифры (0-9)
  - Специальные символы (!@#$%^&*)

- Запрещено использовать:
  - Личные данные (ФИО, дата рождения)
  - Словарные слова
  - Последовательности символов (12345, qwerty)
  - Старые пароли с незначительными изменениями

2. Примеры надежных паролей:

- Допустимо: "Sch00l#2024!"
- Недопустимо: "password123"

3. Правила хранения паролей:
- Не записывать пароли на бумажных носителях
- Не сохранять пароли в браузере
- Не передавать пароли третьим лицам
- Не использовать один пароль для разных систем
- Обязательная смена пароля каждые 90 дней

4. Рекомендуемые инструменты:
- Менеджеры паролей (KeePass, LastPass)
- Двухфакторная аутентификация (где доступно)

ПРИЛОЖЕНИЕ 3
к Порядку осуществления информационной безопасности
МАОУ «Школа № 5 им. И.О. Родобольского»

ФОРМА ЖУРНАЛА УЧЕТА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дата и время	Описание инцидента	Затронутые системы	Принятые меры	Исполнитель	Статус
15.09.2024 10:30	*Попытка несанкционированного доступа к электронному журналу*	*Электронный журнал*	*Блокировка учетной записи, смена пароля*	*Петров И.И.*	*Решен*
20.09.2024 14:15	*Обнаружение вирусного ПО на рабочей станции*	*Компьютер в кабинете информатики*	*Изоляция от сети, лечение антивирусом*	*Сидоров А.В.*	*В работе*

ПРИЛОЖЕНИЕ 4
к Порядку осуществления информационной безопасности
МАОУ «Школа № 5 им. И.О. Родобольского»

РЕГЛАМЕНТ ДЕЙСТВИЙ ПРИ ОБНАРУЖЕНИИ НСД

1. Первоочередные действия:
1.1. Немедленно прекратить работу с компрометированной системой
1.2. Известить системного администратора по телефону
1.3. Зафиксировать время обнаружения инцидента

2. Действия системного администратора:
2.1. Изолировать зараженную систему от сети
2.2. Заблокировать учетные записи, с которых осуществлен НСД
2.3. Сохранить доказательства инцидента
2.4. Уведомить руководителя организации

3. Восстановительные мероприятия:

3.1. Провести антивирусную проверку
3.2. Восстановить данные из резервной копии
3.3. Проанализировать причины инцидента
3.4. Внести корректировки в систему защиты

4. Документирование:
4.1. Внести запись в Журнал учета инцидентов
4.2. Составить отчет об инциденте

ПРИЛОЖЕНИЕ 5
к Порядку осуществления информационной безопасности
МАОУ «Школа № 5 им. И.О. Родобольского»

ПОЛИТИКА ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ И ИНТЕРНЕТ-РЕСУРСОВ

1. Правила использования электронной почты:
- Запрещена передача конфиденциальной информации без шифрования
- Обязательное использование служебной почты для рабочей переписки
- Запрещено открывать подозрительные вложения
- Обязательная проверка антивирусом всех вложений

2. Правила использования интернет-ресурсов:
- Запрещен доступ к ресурсам, не связанным с образовательной деятельностью
- Запрещено использование анонимайзеров
- Ограничение доступа к социальным сетям в рабочее время
- Запрещено скачивание и распространение пиратского контента

3. Мониторинг и контроль:
- Осуществляется фильтрация нежелательного контента
- Проводится выборочная проверка электронной переписки

4. Ответственность за нарушения:
- Дисциплинарная ответственность согласно ТК РФ
- Ограничение доступа к информационным ресурсам
- Обязательное прохождение дополнительного инструктажа