Соловьева Светлана Анатольевна

Соловьева Светлана Анатольевна
O="МОУ ""Зашижемская средняя общеобразовательная школа""", CN=Соловьева Светлана Анатольевна, E=zashijemessh@mail.ru
Я подтверждаю этот документ своей удостоверяющей подписью
2026.10.20 19:41:19+03'00'

Утверждаю:
_____ С.А. Соловьева
«4» сентября 2026 года

План работы по профилактике безопасного поведения в сети Интернет для школьников

План рассчитан на учебный год и учитывает специфику сельской школы: ограниченный доступ к высокоскоростному интернету, разновозрастные классы в одном кабинете, возможную нехватку узкопрофильных специалистов. Мероприятия дифференцированы по возрастным группам: 1–4 классы, 5–7 классы, 8–11 классы.

Организационный блок (реализуется администрацией школы)

- **Разработка и утверждение локальных актов** (положение об информационной безопасности, регламент использования школьных устройств и сети).
  Срок: август–сентябрь. Ответственный: администрация.
- **Назначение ответственного за информационную безопасность** (учитель информатики).

Работа с педагогическим коллективом

- **Семинар «Современные интернет-угрозы и возрастные особенности восприятия рисков детьми».**
  Срок: сентябрь. Ответственный: ответственный за ИБ + приглашённый специалист (при возможности).
  Содержание: краткий обзор фишинга, кибербуллинга, груминга, мошенничества, опасных челленджей; разбор, как эти угрозы выглядят для разных возрастов.
- **Методические консультации «Как интегрировать темы цифровой безопасности в уроки».**
  Срок: октябрь. Ответственный: завуч, учитель информатики.
  Примеры интеграции: на уроках окружающего мира (1–4) — «Правила общения в сети», на обществознании (5–9) — «Права и ответственность в интернете», на информатике — «Пароли и двухфакторная аутентификация».

- **Регулярные совещания (1 раз в четверть)** по анализу инцидентов и корректировке плана. Ответственный: замдиректора по УВР.

Работа с учащимися

1–4 классы (акцент на базовые правила и доверительный формат)

- **Серия игровых классных часов «Путешествие в безопасный интернет» (4 занятия по 30–40 минут).** Темы: «Кто такие незнакомцы в сети?», «Что нельзя публиковать о себе», «К кому обратиться, если что-то пугает в интернете», «Хорошие и плохие сайты». Формат: сказки, комиксы, мини-квесты, раскраски с правилами. Срок: 1 раз в месяц (сентябрь–декабрь). Ответственные: классные руководители.
- **Конкурс рисунков и мини-комиксов «Мой безопасный интернет».** Срок: ноябрь. Ответственные: учителя начальных классов, педагог-организатор.
- **Просмотр и обсуждение коротких мультфильмов/роликов** (серии «Фиксики», «Смешарики: Азбука безопасности» и аналоги). Срок: в рамках классных часов.

5–7 классы (акцент на распознавание угроз и критическое мышление)

- **Практикум «Проверяем информацию: фейк или правда?».** На реальных примерах (новости, посты в соцсетях) дети учатся замечать признаки фейков: отсутствие источников, эмоциональные заголовки, сомнительные ссылки. Срок: октябрь. Ответственные: учитель информатики + классный руководитель.
- **Ролевая игра «Чат: кто перед тобой?»**. Моделирование ситуаций: незнакомец предлагает «крутые» задания, просит фото, обещает приз за переход по ссылке. Дети учатся алгоритмам отказа и обращения за помощью. Срок: декабрь. Ответственные: классный руководитель, педагог-психолог.
- **Мини-проект «Памятка для младших школьников».** Старшие ученики создают простые памятки (текст + иллюстрации) для 1–4 классов. Срок: январь–февраль. Ответственные: классные руководители, библиотекарь.

8–11 классы (акцент на самостоятельность, правовые последствия, защиту данных)

- **Деловая игра «Расследование цифрового следа».** Разбор кейсов: как личная информация из соцсетей используется мошенниками, как формируется цифровой след, какие данные нельзя публиковать. Практическое задание: проверить настройки приватности

в популярных соцсетях. Срок: октябрь–ноябрь. Ответственные: учитель информатики, классный руководитель.

- **Встреча/онлайн-лекция с юристом или сотрудником полиции** (по возможности) на тему «Правонарушения в сети: ответственность и последствия». Срок: февраль. Ответственные: администрация, классные руководители.
- **Проект «Безопасный аккаунт: от пароля до двухфакторной аутентификации».**
  Учащиеся разрабатывают чек-лист безопасности для своих аккаунтов (сложные пароли, резервные коды, проверка ссылок). Лучшие работы размещаются на стенде и в школьном чате. Срок: март–апрель. Ответственные: учитель информатики.

Работа с родителями

- **Родительское собрание «Цифровая безопасность ребёнка: что важно знать родителям».**
  Темы: возрастные риски, настройки родительского контроля, признаки тревожного поведения, куда обращаться при инцидентах. Срок: сентябрь. Ответственные: замдиректора, педагог-психолог, классный руководитель.
- **Ежемесячные короткие памятки в родительские чаты** (1 страница, 3–5 пунктов) по актуальным темам: «Как распознать кибербуллинг», «Что делать, если ребёнок получил подозрительное сообщение», «Настройки приватности в мессенджерах». Срок: ежемесячно. Ответственные: ответственный за ИБ, классные руководители.
- **Индивидуальные консультации** для родителей по настройке родительского контроля и фильтрации на домашних устройствах. Срок: по запросу. Ответственные: IT-специалист школы, классный руководитель.

Психолого-педагогическая поддержка и реагирование

- **Создание «ящика доверия» и информирование детей о каналах помощи**: школьный психолог, горячая линия для детей (8-800-2000-122). Срок: сентябрь. Ответственные: педагог-психолог, администрация.
- **Алгоритм действий при выявлении инцидента** (кибербуллинг, груминг, опасный контент): фиксация, беседа с ребёнком, информирование родителей, при необходимости — обращение в правоохранительные органы. Срок: утвердить до 1 сентября. Ответственные: администрация, педагог-психолог.

- **Групповые занятия с психологом** для детей, столкнувшихся с кибербуллингом или стрессом из-за онлайн-угроз. Срок: по факту выявления. Ответственные: педагог-психолог.

Просветительские и внешние мероприятия

- **Участие в «Уроке цифры» и «Неделе безопасного интернета».** Срок: согласно всероссийскому графику (обычно октябрь–ноябрь). Ответственные: учитель информатики, классные руководители.
- **Сотрудничество с местной библиотекой и ДК**: организация совместных выставок, викторин, кинопоказов по теме цифровой безопасности. Срок: в течение года. Ответственные: библиотекарь, педагог-организатор.

Контроль и оценка эффективности

- **Анкетирование учащихся 1 раз в полугодие** (простые вопросы: «Знаешь ли ты, куда сообщить, если в сети что-то пугает?», «Как ты поступаешь, если незнакомец пишет в чате?», «Что такое двухфакторная аутентификация?»). Срок: декабрь, май. Ответственные: педагог-психолог, классные руководители.
- **Анализ обращений в «ящик доверия» и инцидентов** (количество, типы, скорость реагирования). Срок: ежеквартально. Ответственные: ответственный за ИБ, администрация.
- **Отчёт по итогам года** с выводами и корректировками плана на следующий год. Срок: май. Ответственные: замдиректора по УВР, ответственный за ИБ.