<u>МБОУ СОШ № 5 с. Иглино</u>

Справка по проведению уроков «Цифровой гигиены»

№ п/п	Наименование образовательного учреждения	Количество обучающихся (всего)	Класс (например 2А, 2Б, 3А, 3Б, 3В)	Количество участвующих в «уроке гигиены»	Процент участников
1	МБОУ СОШ № 5 с. Иглино	1820	3,4г,д,е,5а,б,6в,г,7в, 8-11 классы	787	43,24%

19-23 января в МБОУ СОШ № 5 с. Иглино проходили уроки по "Цифровой гигиены" по теме " Угрозы информационной безопасности: атаки, связанные с компьютерной инженерией, способы выявления наличия вредоносных кодов на устройствах, действия при их обнаружении".

В уроках были рассмотрены понятия:

- **Вредоносное программное обеспечение**. Злоумышленники специально создают заражённые программы, чтобы получить доступ к чужой системе. Некоторые виды вредоносного ПО:
    - **Программы-вымогатели** — блокируют ПО, а злоумышленники просят выкуп за получение доступа к данным.
    - **Программы-шифровальщики** — кодируют файлы, делая их недоступными.
    - **Компьютерные черви** — проникают в устройство и копируют сами себя, в результате чего распространяются по системе.
    - **Трояны** — выглядят как лицензированное ПО и незаметно наносят вред системе.
- **Сетевые атаки и перехват данных**. Например, атаки, когда злоумышленник вмешивается в обмен данными, приводящие к перенаправлению трафика.
- **Атаки с физическим доступом**. Злоумышленники получают непосредственный доступ к устройствам и информации: подключение внешних заражённых носителей, визуальный контроль за экраном устройства, кража оборудования, носителей информации.

В уроках были рассмотрены меры по обеспечению безопасности:

- **Использование антивирусного программного обеспечения**. Оно выполняет регулярную автоматическую проверку устройства по расписанию, обнаруживает и удаляет вредоносные программы. Некоторые методы анализа:
    - **Сканирование структуры файлов** без их выполнения — антивирус сопоставляет бинарные инструкции, строки кода, импортируемые библиотеки с базами сигнатур и хешей.

    - **Динамический анализ** — образец оценивают по его поведению — в действующей системе или в изолированной среде.
    - **Эвристический анализ** — выявляет вредоносные объекты по их поведению и структуре файла, отслеживает характерные признаки подозрительной активности.
- **Анализ трафика** — когда система обнаруживает подозрительный файл, она может быстро проверить его через облачный сервис, который анализирует объект с учётом последних обновлений и данных от других пользователей.
- **Признаки заражения** — снижение производительности устройства, изменение домашней страницы в браузере, частые всплывающие окна с рекламой, проблемы с загрузкой операционной системы или подключением к интернету.

В уроках были рассмотрены действия при обнаружении вредоносных программ или файлов на устройствах:

- **Отключить устройство от интернета** — это предотвратит отправку большего количества личных данных злоумышленникам.
- **Удалить необычные файлы и приложения** — они могут быть замаскированным вредоносным ПО.
- **Включить безопасный режим** — на большинстве устройств есть функция, которая позволяет загружать только минимально необходимое программное обеспечение.
- **Сбросить устройство к заводским настройкам** — перед этим нужно убедиться, что все данные сохранены в резервной копии, иначе они будут утеряны.
- **Поменять пароли** от учётных записей, если есть подозрение на то, что они могли быть украдены.
- **Регулярно делать резервные копии** важных данных и проверять их работоспособность, чтобы информацию можно было восстановить в случае заражения устройства.

В уроках были использованы материалы:

- **Видеоролик «Виды информационных угроз и как себя защитить от них»** — помогает объяснить виды угроз и методы защиты.
- **Статью «Что такое вредоносный код?»** — даёт определение вредоносного кода и примеры угроз.
- **Методические рекомендации по защите мобильных устройств** — например, правила проверки разрешений приложений, загрузки приложений только из официальных магазинов, настройки биометрической аутентификации.

Важно подчеркнуть, что абсолютной безопасности в цифровом мире не существует, но соблюдение базовых правил цифровой гигиены помогает снизить риски столкновения с киберугрозами.

Справку подготовила заместитель директора УР Гиндуллина М.И.