Напомним, что в начале этого года ВЦИОМ совместно с Альянсом по защите детей в цифровой среде провёл опрос родителей детей до 14 лет. Согласно его результатам, 91% родителей разрешают своим детям пользоваться «умной» колонкой как минимум раз в неделю, из них 54% — ежедневно, а 33% — несколько раз в неделю.

Учитывая высокую вовлечённость детей в использование голосовых помощников, важно понимать потенциальные риски и знать меры защиты.

1. Защита конфиденциальности при сборе данных.

Компании собирают данные о предпочтениях (любимая музыка, вопросы, которые вы или ваш ребенок задаете, интересы). Это используется для таргетированной рекламы и создания профиля пользователя.

Решение - Отключите персонализированные ответы.

Это не даст колонке использовать историю поисков и запросов для формирования ответов, что повышает конфиденциальность.

В приложении: —> Перейти в настройки: нажать «→ ». —>Отключить опцию «Персонализированное общение».

Чтобы очистить контекст, нажать «Удалить контекст» и подтвердить удаление.

2. Неподходящий по возрасту контент: Музыка с ненормативной лексикой, подкасты или новости на тревожные темы, ответы на вопросы, которые ребенок не готов воспринимать.

— Обязательно включите «Детский режим».

— Убедитесь, что активированы фильтры контента и безопасный поиск.

— Проверьте, какие навыки/действия разрешены: отключите всё стороннее, кроме проверенных.

→ Настройки профиля → «Детский режим» → выбрать возраст ребёнка → включить фильтрацию.

3. Голосовые покупки и управление «умным домом»

Ребёнок может случайно оформить заказ или включить опасные устройства (замки, электроприборы).

— Отключите голосовые покупки в настройках аккаунта.

— В «умном доме» запретите колонке управлять критичными устройствами через настройки в приложении.

4. Также через приложение можно настроить оповещения о попытках доступа к запрещённому контенту, продолжительности использования устройства и других значимых событиях.

Ниже - общие рекомендации по настройкам безопасности умных устройств:

- Правильно настройте домашнюю Wi-Fi сеть: используйте надёжный пароль и надёжное шифрование.
- Сразу после настройки устройства измените его имя — чтобы киберпреступникам было сложнее определить модель.
- Измените установленный по умолчанию пароль. Создайте надёжный пароль и регулярно его меняйте. Не используйте одинаковые пароли на разных устройствах.
- Если есть возможность, используйте многофакторную аутентификацию для доступа к устройству.
- Вовремя устанавливайте обновления программного обеспечения вашего устройства.
- Внимательно прочитайте политику конфиденциальности, особенно в отношении использования личных данных.
- Проверьте в настройках параметры конфиденциальности, отключите те разрешения, которые считаете лишними.

Научите детей обращаться к вам в случае, если колонка сказала что-то странное или пугающее и обязательно рассказывайте детям о правилах цифровой гигиены, дайте понять, что колонка — машина, а не человек.