

Мобильные приложения монетизируют наши данные. Как сохранить приватность?

Макарова Анастасия, Дорошко Ксения, Казакова София, Ульянова Софья, II курс, филиал БГТУ «ВитГТК», Витебск.

Научный руководитель: Аювджи О. В., преподаватель высшей квалификационной категории.

Актуальность исследования:

Бесплатные приложения стали «бесплатными» неслучайно: они платят за свою работу вашими персональными данными. Каждое второе приложение просит доступ к геолокации, микрофону и контактам, собирая цифровой портрет пользователя. Это основа современной экономики — данные стали ценнее денег. Пользователи, выбирая удобство, редко читают многостраничные политики конфиденциальности и не осознают, какую информацию отдают. Даже строгие законы лишь частично ограничивают этот процесс, но не останавливают сбор данных полностью.

Задачи проекта:

1. Провести сравнительный анализ бизнес-моделей и политик сбора данных на примере двух популярных приложений с разной философией, выделив ключевые различия в подходах к приватности пользователя.
2. Создать наглядную схему распространения персональных данных от мобильного устройства пользователя до конечных потребителей.
3. Разработать и визуально оформить практико-ориентированную памятку (чек-лист) по цифровой гигиене.



Объект исследования:

Данные пользователя

Предмет исследования:

Цифровой след

Информационная база исследования:

1. Первичные источники:

Политики конфиденциальности Telegram и TikTok.

2. Вторичные источники:

Аналитика рынка данных (Statista, App Annie), экспертные статьи и расследования (Habr, Wired).

3. Практические данные:

Аудит разрешений приложений в смартфоне, данные об утечках (Have I Been Pwned).

2. Для образовательных проектов

Материалы исследования станут основой для уроков и лекций по цифровой грамотности. Схемы и таблицы наглядно покажут, как устроена слежка в разных приложениях, помогая развивать критическое мышление при использовании технологий.

Методы исследования:

1. Сравнительный анализ
2. Системный анализ
3. Анализ документов
4. Моделирование
5. Обобщение

Практическая ценность и возможное использование результатов работы:

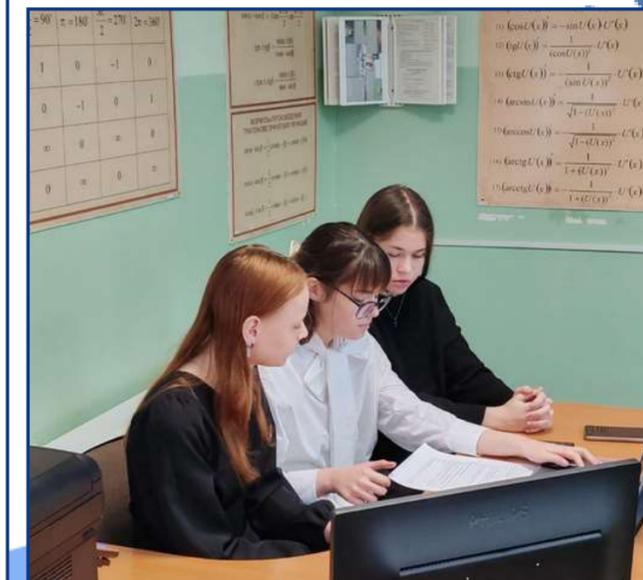
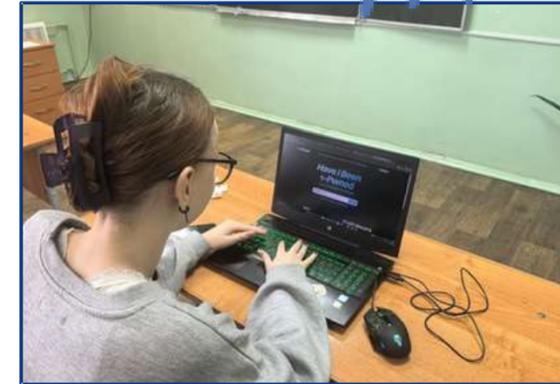
Результаты данного исследования имеют конкретную пользу для трёх ключевых групп.

1. Для пользователей соцсетей

Вы получите простую инструкцию по цифровой защите: как настроить приватность, чтобы вас меньше отслеживали. Понимание работы алгоритмов поможет осознанно управлять своей лентой, а не зависеть от настроения системы.

3. Для законодателей и правозащитников

Исследование выявит правовые пробелы в регулировании сбора поведенческих и психологических данных. Выводы послужат основой для разработки законов, требующих от платформ большей прозрачности и ограничивающих скрытое манипулирование пользователями.



7 правил цифровой гигиены

Безопасность - это система привычек. Начните с 2FA и менеджера паролей, остальные правила постепенно усилят вашу защиту.

✉ ДРОБЛЕНИЕ ПОЧТЫ.

Создайте несколько ящиков для разных целей: личный, для регистраций, «мусорный». Это изолирует риски - утечка данных с форума не затронет ваш банковский аккаунт.

📧 ПРЕДПОЧИТАЙТЕ EMAIL НОМЕРУ ТЕЛЕФОНА.

При регистрации везде, где возможно, используйте почту. Номер телефона - ключ к SMS-банкингу и его сложнее сменить при утечке.

🔑 МЕНЕДЖЕР ПАРОЛЕЙ + 2FA.

Никогда не повторяйте пароли. Доверьте генерацию и хранение менеджеру (Google/Apple или Bitwarden). Второй обязательный шаг - включите двойную проверку везде (например: после ввода пароля сайт будет запрашивать дополнительный код, который приходит только на ваш телефон.)

⚙ ЖЁСТКИЙ КОНТРОЛЬ РАЗРЕШЕНИЙ ПРИЛОЖЕНИЙ.

Регулярно проверяйте, какие доступы есть у программ. Отключайте геолокацию, микрофон и контакты у приложений, которым это не нужно для работы.

🕸 ЗДОРОВЫЙ СКЕПСИС К VPN И РЕКЛАМЕ.

Бесплатные VPN часто продают данные пользователей. Не доверяйте агрессивной рекламе - проверяйте сервисы через независимые обзоры.

🔄 АВТОМАТИЧЕСКИЕ ОБНОВЛЕНИЯ.

Включите автообновления ОС и приложений. Большинство обновлений содержат критические исправления уязвимостей, а не только новые функции.

🛡 РЕГУЛЯРНАЯ ПРОВЕРКА НА УТЕЧКИ ДАННЫХ.

Используйте сервисы вроде Have I Been Pwned для проверки email. При обнаружении утечки немедленно меняйте пароли на затронутых сервисах. Отсканируйте этот QR-код, чтобы получить инструкцию по работе с сайтом.



СРАВНИТЕЛЬНАЯ ТАБЛИЦА ПО СБОРУ ДАННЫХ ТIKТОК И TELEGRAM

Источник данных	Tik Tok	Telegram
Контент в приложении	Всё: что смотрите, лайкаете, комментируете	Минимум: только для работы сервиса
Техника устройства	Подробно: модель, ОС, сеть, рекламный ID	Базово: только для подключения
Метаданные	Анализ паттернов: как скроллите, время сессий	Практически нет
Трекинг вне платформ	Есть: через TikTok Pixel на сайтах	Нет
Контакты	Анализирует для рекомендаций друзей	Только синхронизация
Геолокация	Точно по GPS (при разрешении)	По IP (страна/город)
Аудио/видео	Только то, что публикуете в приложении	Только то, что отправляете
Бизнес-модель	Реклама на основе данных	Подписки и экосистема