



ЦИФРОВЫЕ СЛЕДЫ

Кто ими пользуется
и как себя защитить



Спикер

● **Никифоров Андрей**

Эксперт по защите персональных данных



ЦИФРОВЫЕ СЛЕДЫ

ТЕОРИЯ



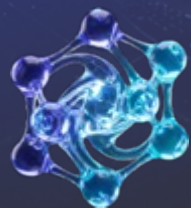
Цифровой след

Что это

Цифровой след

Это вся информация, которую пользователь оставляет в интернете.

Например: история посещённых сайтов и поисковые запросы, сообщения в мессенджерах, посты и лайки в соцсетях, геолокация, данные транзакций и файлы в облаке



Полностью стереть цифровой след практически невозможно

Интернет помнит всё

Цифровой след россиян

225 млн

Активных подключённых мобильных телефонов, на конец 2025г.

По данным Datareportal

136 млн

Человек используют интернет, на конец 2025г.

По данным Datareportal

106 млн

Пользователей социальных сетей, на Октябрь 2025г.

По данным Datareportal

Цифровой след

Виды

Активный

Данные, которые пользователь сознательно оставляет в интернете.

Посты, фото и комментарии в соцсетях, видео, статьи и т. д.

Пассивный

Информация, которую пользователь выкладывать не собирался.

Список посещённых сайтов, поисковые запросы, IP-адреса и геолокационные данные

Сайты, сервисы, устройства и приложения собирают такую информацию автоматически, например при помощи cookies



Персональные данные

Это важно знать

Персональные данные

Это любая информация, благодаря которой можно идентифицировать конкретного человека



Хобби

Номер телефона

Документы

Особенности внешности

ФИО

Возраст

Адрес

Имидж и стиль

Кто использует ваш цифровой след

Провайдеры

Компании

Злоумышленники

Гос. органы

Поисковые
системы



Почему оставлять много цифровых следов **опасно**

Потеря приватности

Злоумышленники могут использовать данные в своих целях, в том числе незаконных

Кража личности

Шантаж

Слежка

Потеря репутации

Старые забытые публикации могут всплыть через годы и стать причиной социальных последствий

Увольнение

Подрыв доверия

Физическая угроза

Захват личных устройств

Успешная атака мошенников может привести к попаданию вирусов на ваш девайс

Шифрование данных

Блокировка

Потеря денег

ЦИФРОВЫЕ СЛЕДЫ ПОСЛЕДСТВИЯ



Базы США в Афганистане

- В январе 2018 года австралийский студент обнаружил, фитнес-приложение Strava раскрывает местоположение пользователей
- Карта, составленная на основе данных GPS-трекеров 27 миллионов пользователей за 2015–2017 годы
- В зонах, где ярко подсвечивалась активность пользователей оказались военные базы США и их союзников.
- Подозрение вызвало то, что на этих участках местное население такими устройствами как правило не пользуется — в пустынях Сирии, Ирака и Афганистана



Скандал с Cambridge Analytica

- Британская аналитическая компания через приложение-опросник незаконно собрала персональные данные около 87 миллионов пользователей соцсети
- Приложение собирало информацию не только о тех, кто его проходил, но и о всех друзьях этих пользователей
- Компания использовала эту информацию для продвижения политической рекламы, в том числе президентской кампании Дональда Трампа в 2016 году



Взлом Ashley Madison

- В июле 2015 года хакерская группа взломала серверы сайта знакомств Ashley Madison
- В результате данные 37 миллионов пользователей попали в сеть
- Раскрытая информация содержала чувствительную информацию, личные данные и в последствии привела к миллионам разрушенных семей





ЦИФРОВЫЕ СЛЕДЫ

СХЕМЫ МОШЕННИЧЕСТВА

Фейковый друг

Что делать, если просят данные или деньги

- Не действуйте на эмоциях
- Позвоните другу, спросите, действительно ли ЕМУ нужна помощь
- Не переходите по ссылкам и не отправляйте данные и деньги, если не удостоверились в личности человека



Бесплатный сыр

Что делать, если попадаете конкурс в интернете

- Не участвуйте в сомнительных акциях — кто бы о них ни рассказывал
- Не верьте тем, кто предлагает заплатить, чтобы получить приз
- Если вы видите соблазнительный розыгрыш подарков от публичной личности, проверьте его аккаунт



Знакомьтесь, мошенник

Что делать, если с вами хотят познакомиться

- Не делитесь конфиденциальной информацией
- Не отправляйте собеседнику деньги
- Не переходите по незнакомым ссылкам, которые вам отправляет собеседник
- Не бойтесь проявлять инициативу и расспрашивать нового приятеля о его жизни
- Предложите связаться по видеосвязи, чтобы убедиться в личности человека



ЦИФРОВЫЕ СЛЕДЫ

ПРАВИЛА ЗАЩИТЫ



Читайте согласия

Эти документы определяют судьбу
ваших персональных данных

Согласие на обработку персональных данных

Письменное разрешение гражданина Российской Федерации, которое он дает компании на получение, сбор, хранение и использование личных данных

Используй Ctrl/cmd + F для
поиска нужной информации
в документах



Ограничьте лишние данные

Интернет – это общественное место

Используйте настройки приватности

В настройках соцсетей и мессенджеров установите, кто может видеть вашу личную информацию

Не используйте соцсети как облако

Документам, адресам, паролям – не место в соцсетях. Хранение данных в переписках может привести к их утечке

Добавляйте в друзья только знакомых

Удостоверьтесь, что в списке друзей в соцсети нет незнакомых вам лиц и регулярно их перепроверяйте

Цифровая гигиена

Защита данных – непрерывный процесс

Сложные пароли

Они должны состоять из 12+ букв цифр и символов. Не используйте один и тот же пароль на разных аккаунтах

Двухфакторная аутентификация

Используйте эту функцию на всех аккаунтах, где это доступно

Фишинг

Остерегайтесь фишинга – перед тем, как вводить персональные данные, убедитесь, что это официальный сайт



Цифровая гигиена

Общие правила

● Не раскрывайте личную информацию незнакомцам, даже если они очень убедительны

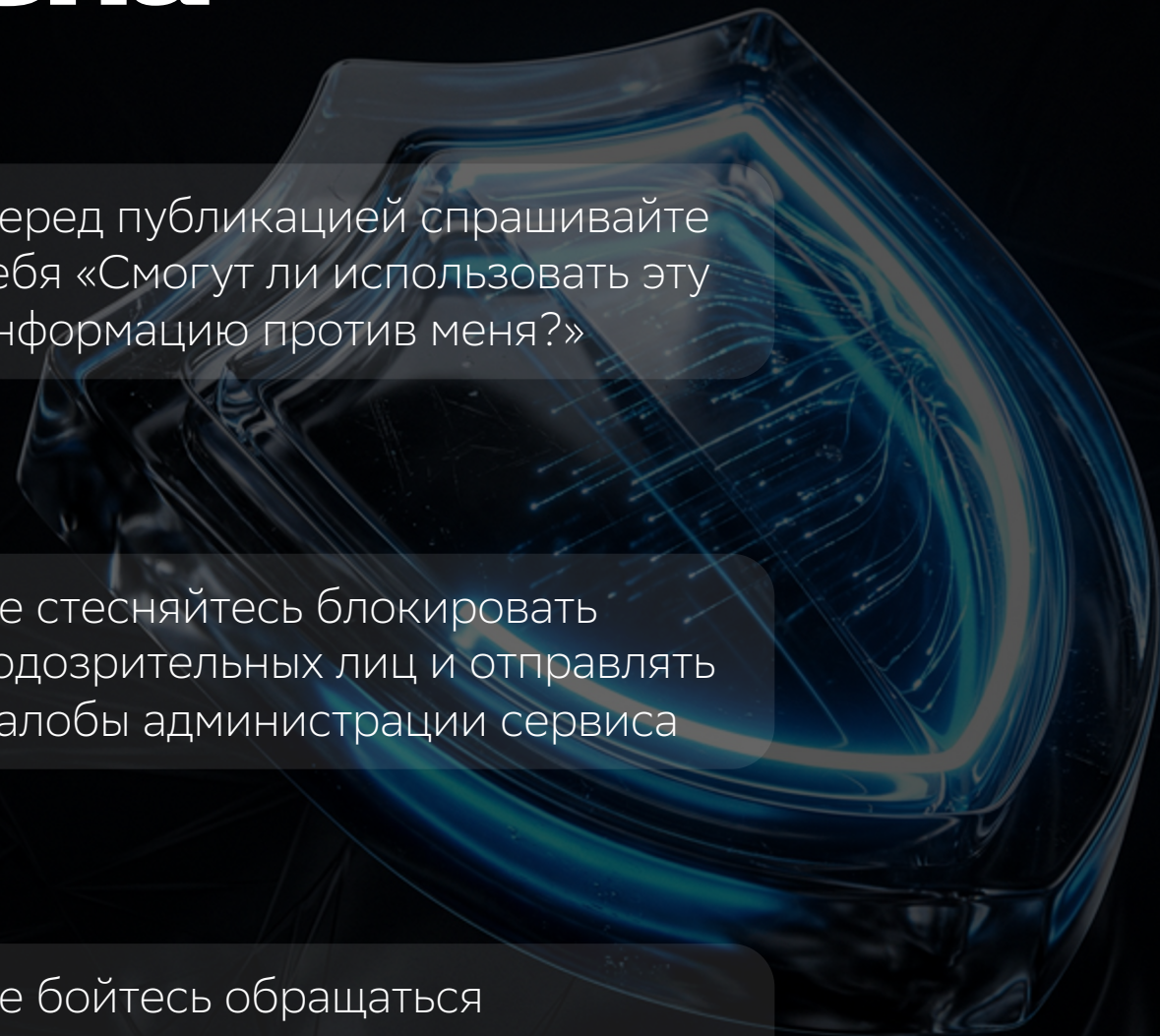
● Не переходите по подозрительным ссылкам, вводите адрес сайта самостоятельно

● Не ведите переговоры с мошенниками – положите трубку

● Перед публикацией спрашивайте себя «Смогут ли использовать эту информацию против меня?»

● Не стесняйтесь блокировать подозрительных лиц и отправлять жалобы администрации сервиса

● Не бойтесь обращаться за помощью к друзьям и близким





**БЕРЕГИТЕ СЕБЯ И СВОИ
ПЕРСОНАЛЬНЫЕ
ДАННЫЕ**