ФИНАНСОВЫЙ УНИВЕРСИТЕТ
1919
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный методический центр по финансовой грамотности населения на базе Институт финансовой грамотности Финуниверситета

Тема: Цифровой след в платежной сфере: способы снижения рисков

Спикер: Трофимов Дмитрий Викторович

к.э.н., доцент Кафедры банковского дела и монетарного регулирования, эксперт ФМЦ ИФГ

ЦИФРОВОЙ СЛЕД

Цифровой след (или «цифровая тень», «цифровой отпечаток») — это совокупность данных, которые пользователь сознательно или неосознанно оставляет в цифровой среде в процессе своей деятельности. Это все записи о наших действиях, предпочтениях, перемещениях и взаимодействиях, которые фиксируются устройствами, платформами и сервисами.

- **Активные (сознательные) следы:** данные, которые пользователь целенаправленно и добровольно предоставляет.

- **Пассивные (фоновые) следы**: данные, собираемые автоматически без явных действий пользователя.
  - Лог-файлы и метаданные
  - Данные от устройств (IoT)
  - Данные о транзакциях:

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

КТО И КАК СОБИРАЕТ ЦИФРОВЫЕ СЛЕДЫ

Субъекты сбора:

- Корпорации (коммерческие компании):
  - Технологические гиганты и платформы
    Телекоммуникационные операторы
  - Финансовый сектор
  - Ритейл
- Государство
- Злоумышленники

Основные технологии и методы сбора:

- Cookies (куки)
- Смартфон
  - Геолокация (GPS, соты)
  - Данные приложений
  - Датчики движения.
- Прочие устройства Интернета вещей (IoT)
- Прямой ввод через формы

РЫНОК ДАННЫХ

Рынок данных — это система экономических отношений, связанных со сбором, обработкой, анализом и монетизацией цифровых следов.

«Данные» — любая информация, которую можно собрать и обработать для получения аналитической или прогностической ценности.

Даркнет (Darknet) — это скрытая часть интернета, недоступная через обычные браузеры и поисковики, требующая специальных программ для доступа, что обеспечивает высокую анонимность пользователей через шифрование и перенаправление трафика, и используется как для законных целей, так и для незаконной деятельности (торговля украденными данными, запрещенными товарами).

КТО ПРИСУТСТВУЕТ НА РЫНКЕ

- **Data Brokers (брокеры данных)** — компании, которые специализируются на сборе информации из множества открытых и закрытых источников, её очистке, агрегации и формировании готовых профилей для продажи.
- **DMP (Data Management Platform)** — технологические платформы для сбора и управления большими массивами данных из разных источников (например, «Яндекс.Audience», VK Ads).
- **Крупные цифровые экосистемы («Яндекс», «Сбер», VK)** — являются одновременно и сборщиками, и мощными обработчиками, и потребителями своих же данных.

КТО ПРИСУТСТВУЕТ НА РЫНКЕ

Эффект накопления:

В связке с:

- банками,
- операторами связи,
- платформами ЦБ,
- МВД и другими госорганами

возникает сквозная корреляция данных:

- номер телефона ↔ банковская карта;
- IP-адрес ↔ онлайн-банкинг;
- устройство ↔ финансовые операции;
- поведенческие паттерны ↔ риск-оценка.

COOKIES — НАЧАЛО ОТСЛЕЖИВАНИЯ

Сессионные куки — это временные куки, которые исчезают, как только вы закрываете браузер.

Постоянные куки — они хранятся месяцы или даже годы.

Third-party куки — это самые коварные. Это куки от компаний, которых вы не видите. Например, вы заходите на новостной сайт, а там реклама от Google. Google ставит свой куки и начинает отслеживать вас не только на этом сайте, но и на сотнях других сайтов, где есть его объявления.

МАСШТАБ ОТСЛЕЖИВАНИЯ

Знаете ли вы, что 61% всех куки на интернете — это third-party куки? То есть куки от компаний, которые вам не нужны.

Google Analytics установлена на более чем 60% веб-сайтов. Это значит, что Google видит, что вы делаете на большинстве сайтов, которые вы посещаете. Они видят, где вы нажали, сколько времени вы потратили, что вы купили.

Сохраняется всё: история поиска, клики, время на странице, ваши покупки, личная информация.

СМАРТФОН — ГЛАВНЫЙ ВРАГ ПРИВАТНОСТИ

Ваш смартфон — это архив всех ваших данных.

- Геолокация. Ваш телефон ВСЕГДА знает, где вы находитесь. GPS, WiFi сети, даже Bluetooth маячки в магазинах — это всё используется.
- IDFA и AAID. Это уникальные идентификаторы вашего телефона. IDFA — для iPhone, AAID — для Android. Это был придуман для «анонимного» отслеживания.
- Данные сенсоров. В вашем телефоне есть акселерометр и гироскоп.
- Список приложений. Компания видит, какие приложения вы установили. Это уже рассказывает о вас многое.
- Разрешения. Когда приложение просит разрешение на доступ к контактам, календарю, фотографиям — оно может это использовать. И даже если вы запретили доступ к геолокации, приложение может её вычислить по WiFi-сетям, которые оно видит.

ДРУГИЕ СБОРЩИКИ ДАННЫХ

Помимо смартфона, есть и другие устройства, которые собирают данные.

- IoT-устройства. Умная колонка в вашем доме, умные часы, даже холодильник — они все подключены к интернету и отправляют данные компаниям.
- Голосовые помощники. Alexa, Google Assistant, Siri — они слушают вас. Они записывают ваши команды, ваш голос, контекст, в котором вы говорите. Это огромное количество информации о вашем поведении и предпочтениях.
- **Платежные системы.** Каждая ваша покупка записана. История всех покупок — это портрет вашего образа жизни, вашего дохода, вашего здоровья (если вы покупаете лекарства).
- Социальные сети. На большинстве сайтов стоят пиксели от Facebook, Instagram. Даже если вы не в соцсети, они знают, что вы там были.

ЧТО ТАКОЕ ЦИФРОВОЙ ПРОФИЛЬ

Итак, когда компания собирает все эти данные — куки, геолокацию, IDFA, покупки, голосовые команды — она создаёт цифровой профиль. Это не просто база данных. Это полный портрет вас как человека.

Сюда входит:

- Демография. Компании знают ваш возраст, пол, примерный доход, семейный статус. Всё это вычисляется из данных.
- Интересы и хобби. Вы интересуетесь спортом? Искусством? Технологией? Компания знает из того, какие сайты вы посещаете, какие видео смотрите, какие приложения используете.
- Поведение. Как вы совершаете покупки? Вы импульсивны или вдумчивы? Вы доверяете рекламе или ищете отзывы? Компания знает.
- Кредитоспособность. На основе вашего поведения компания может оценить, насколько вы надёжны. Сколько долгов у вас есть? Насколько быстро вы платите?

Этот профиль используется для таргетирования рекламы, для оценки кредитного риска, для назначения цен (да, вы можете платить больше, если алгоритм знает, что вы можете себе это позволить), и даже для предсказания вашего поведения.

ЗАКЛЮЧЕНИЕ

Вы оставляете следы везде — в браузере, на телефоне, в умных устройствах, в платежных системах.

Эти следы собирают и анализируют компании. Это не огромный заговор — это просто бизнес-модель.

Результат — это ваш цифровой профиль, который используется компаниями для таргетирования, для манипуляции, для предсказания.

Что с этим можно сделать? В первую очередь, быть в курсе. Понимать, как работает эта система. А потом — принимать решения. Отключать куки, удалять приложения, использовать VPN. Это мелко, но это лучше, чем ничего.

«Закон Яровой» (ФЗ-374)

Пакет направлен на противодействие терроризму и экстремизму с использованием интернета, а также на упрощение расследования таких дел. Разработчики подчёркивали, что закон поможет выявлять опасных преступников, и не связан с тотальной слежкой за добропорядочными гражданами.

Положения «пакета Яровой»:

- Ужесточение наказания по экстремистским и террористическим статьям.
- Расширение списка преступлений, по которым уголовная ответственность наступает с 14 лет. К ним, например, отнесли участие в массовых беспорядках.
- Требования к операторам связи и провайдерам.
- Регулирование миссионерской деятельности.

УВЕЛИЧЕНИЕ «ЦИФРОВОГО СЛЕДА»

Федеральный закон № 374-ФЗ («пакет Яровой») ввёл для операторов связи и интернет-сервисов обязанности:

- хранить трафик пользователей:
- содержание сообщений, голос, файлы — до 6 месяцев;
- метаданные (кто, кому, когда, откуда) — до 3 лет;
- обеспечивать расшифровку сообщений по законному запросу уполномоченных органов;
- передавать данные в рамках оперативно-разыскной деятельности.

Что именно формируется

- детализация звонков;
- SMS / мессенджеры (факт и содержание);
- IP-адреса, MAC-адреса, IMEI;
- геолокация;
- время, частота, маршруты коммуникаций.

БД ЦБ «ПРОТИВ МОШЕННИЧЕСТВА

База данных Банка России «О случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента»

Цель базы — противодействовать переводам, которые происходят без согласия клиента, в частности под воздействием злоумышленников.

Ведение базы данных предусмотрено Федеральным законом от 27.06.2011 №161-ФЗ «О национальной платёжной системе». Банки обязаны передавать в Банк России информацию обо всех случаях и попытках таких переводов, в том числе тех, по которым клиенты заявили своё несогласие с их совершением. finstarbank.rucbr.rucbr.ru

С 1 сентября 2025 года в базу данных включаются сведения о мошеннических операциях, связанных с внесением наличных на счета через банкоматы с применением токенизированных (цифровых) карт.

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСЛЕДСТВИЯ ВКЛЮЧЕНИЯ В БАЗУ

Банки вправе или обязаны:

- приостановить операции;
- заблокировать карты;
- ограничить онлайн-банкинг;
- при источнике данных от МВД — блокировка обязательна;
- режим распространяется и на цифровой рубль .

ИСТОЧНИКИ ДАННЫХ

В ЦБ РФ стекается информация от:

- банков и НКО;
- МВД России;
- операторов платёжной инфраструктуры;
- операторов платформы цифрового рубля;
- операторов связи;
- владельцев мессенджеров;
- владельцев сайтов и интернет-платформ.

Какие данные содержатся в базе:

- данные о получателях средств (ФЛ и ЮЛ);
- реквизиты карт, счетов, электронных средств платежа;
- абонентские номера;
- IP-адреса;
- параметры устройств (идентификаторы, совпадения);
- сведения о нетипичном поведении:
  - резкие изменения операций;
  - нетипичные звонки;
  - аномальные сообщения.

ПЛАТФОРМА ЦБ РФ ПО ЮРИДИЧЕСКИМ ЛИЦАМ

«Знай своего клиента» (ЗСК)

Правовая база:

- ФЗ № 115-ФЗ (ПОД/ФТ);
- ФЗ № 86-ФЗ «О Центральном банке РФ».
- Система работает с 1 июля 2022 года.

Суть платформы

ЦБ централизованно аккумулирует данные о:

юридических лицах;

индивидуальных предпринимателях;

присваивает уровень риска:

низкий (зелёный);

средний (жёлтый);

высокий (красный);

информация ежедневно передаётся банкам.

ЕДИНАЯ ПЛАТФОРМА СБОРА И ОБРАБОТКИ ОТЧЕТНОСТИ

«Единая платформа сбора и обработки отчетности» Банка России

Суть

- вся финансовая отчетность компаний концентрируется в ЦБ
- банки, НКО, страховщики, профучастники — в едином контуре
- ЦБ становится центральным узлом данных о бизнесе

ОБЩИЙ ВЫВОД

«Закон Яровой», базы данных и платформы Банка России формируют единое цифровое пространство контроля, где:

- телеком-данные,
- финансовые операции,
- технические параметры,
- поведенческие модели

сопоставляются и анализируются централизованно.

Практическое значение

- рост прозрачности для государства;
- снижение анонимности;
- усиление превентивного контроля;
- формирование долгосрочного цифрового профиля граждан и бизнеса.

ЦИФРОВАЯ ИДЕНТИЧНОСТЬ И БИОМЕТРИЯ

Цифровая идентичность – набор электронных данных, используемый для однозначной идентификации личности в цифровой среде

Пользователь получает преимущества в виде:

- Повышенного удобства (73% называют биометрию «самым удобным способом оплаты»)
- Скорости доступа (Face Pay в метро — 0,3 секунды),
- Возможности пользоваться рядом сервисов без повторной идентификации

Однако он также сталкивается с рисками:

- Невозможность отзыва биометрических данных после утечки
- Потенциальное использование его лица или голоса для создания дипфейков
- Ограничение доступа к сервисам при отказе от регистрации в ЕБС (например, мобильная связь для иностранцев с 1 июля 2025 года)

При этом пользователь не получает доли прибыли, которую генерируют компании на основе его данных

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРОЕКТ ЦБ РФ «АНТИДРОП»

Проект платформы «Антидроп» — это государственная система, которую Банк России (ЦБ РФ) разрабатывает для борьбы с дропперами

Задачи:

- Обмениваться информацией между банками и регулятором о подозрительных клиентах и операциях
- Предотвращать мошенническую активность, связанную с быстрым обналичиванием и переводами, выводом украденных средств и т.п.
- Повысить устойчивость финансового рынка и снизить системные риски, связанные с трансакционной активностью подозрительных клиентов

ФЗ-41 «О БЕЗОПАСНОСТИ РУНЕТА»

- Создаётся государственная информационная система противодействия ИКТ-правонарушениям.
- Цель: выявление, пресечение и предотвращение мошенничества в связи, финансах и интернете
- В системе хранятся данные о лицах и номерах, использованных для противоправных действий
- Пользователи: МВД, ФСБ, СК, Генпрокуратура, ЦБ, банки, операторы связи и др.
- Оператор системы — федеральный орган в сфере ИТ (фактически Минцифры)

ФЗ-41 «О БЕЗОПАСНОСТИ РУНЕТА»

- Теперь банк обязан проверять операции снятия наличных на признаки мошенничества и вправе устанавливать лимиты на переводы: 50000 - 100000
- Банки, агрегаторы, операторы связи обязаны передавать данные силовым органам через единую систему межведомственного электронного взаимодействия
- Это распространяется на: МВД, ФСБ, СК, прокуратуру и органы госохраны
- Запрещено использовать иностранные мессенджеры (по юридическому описанию — WhatsApp, Telegram и аналоги) для информирования граждан: Госорганам, ЦБ, банкам, операторам связи, госкорпорациям, маркетплейсам, крупным интернет-платформам

ФЗ-41 «О БЕЗОПАСНОСТИ РУНЕТА»

- Разрешается и в ряде случаев обязательно использование: ЕСИА (Госуслуги), Единой биометрической системы (ЕБС)
- Обязательно: для микрофинансовых организаций при дистанционных займах и при каждом онлайн-договоре займа (МФО)
- Продавцы маретплейсов идентифицируются через Госуслуги (по желанию — биометрия)
- Массовые/автоматические звонки только с согласия абонента

ФЗ-41 «О БЕЗОПАСНОСТИ РУНЕТА»

- Абонент имеет право: запретить рассылки и массовые звонки и запретить оформление SIM-карт на себя
- Запрещена передача SIM-карты третьим лицам. Разрешено — только: членам семьи, близким родственникам
- Мессенджеры, сайты, хостинг-провайдеры обязаны: взаимодействовать с гос-антифрод-системой; передавать данные о мошенничестве; исполнять ограничения и блокировки.

MAX

- Это российский (государственный) аналог whatsapp и telegram. По сути, от них не отличается ничем. Собирает все те же данные о пользователе, что и другие подобные приложения. Так же как и они может предоставлять данные третьим лицам.
- Ключевое отличие – зарегистрироваться можно только при помощи актуального российского/белорусского номера телефона. Так же государственные органы могут значительно быстрее получить данные о пользователе (особенно, если он совершает что-то незаконное).

VPN

1. Данные, которые видит VPN-провайдер:

- Весь ваш трафик проходит через сервера провайдера
- Ваш реальный IP-адрес
- Время подключения, продолжительность сессий
- При использовании платных VPN — платежная информация

2. Следы на вашем устройстве:

- Логи браузеров (cookie, кеш, история посещений)
- Данные, переданные до активации VPN
- Информация из приложений, которые не используют VPN-туннель
- Цифровые отпечатки браузера (fingerprinting)

3. Поведенческие паттерны:

- Привычки посещения сайтов
- Стиль письма (при анализе текстов)
- Время активности в сети

4. Технические уязвимости:

- Утечки DNS и WebRTC могут раскрыть реальный IP
- При отключении VPN возможна утечка реального адреса
- Мобильные устройства часто переключаются между сетями

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

VPN

5. Юридические аспекты:

- В некоторых странах VPN-провайдеры обязаны хранить логи
- При сотрудничестве с правоохранительными органами провайдер может предоставить данные

6. Метаследы:

- Временные метки вашей онлайн-активности
- Объем передаваемых данных
- Используемые порты и протоколы

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЫВОД: МОЖНО ЛИ ДОВЕРЯТЬ СМАРТФОНУ

Критические факты:

- 83% устройств имеют уязвимости
- 67% пользователей не подозревают о компрометации данных
- iOS и Android одинаково уязвимы (Pegasus, банковские трояны)

Основные векторы атак:

- Уязвимости чипсетов (Qualcomm/Mali)
- Эксплойты в предустановленных приложениях
- Атаки через Bluetooth/Wi-Fi (BlueBorne)
- Физический доступ (1 минута = компрометация)

Опасное поведение пользователей:

- 92% хранят конфиденциальные данные в телефоне
- 78% используют один пароль для всех сервисов
- 63% не проверяют разрешения приложений

5 скрытых угроз:

- Обход 2FA банковскими троянами
- Скрытая активация камеры/микрофона
- Клавиатурные шпионы
- Сбор геоданных без GPS
- Руткиты, переживающие сброс системы

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЫВОД: МОЖНО ЛИ ДОВЕРЯТЬ СМАРТФОНУ

Меры защиты:

- Аппаратные ключи U2F вместо SMS
- Отключение USB-отладки
- Firewall (NetGuard)
- Регулярная проверка администраторов устройства
- Изолированные профили для банковских приложений

Вывод:

Смартфон — потенциально опасный инструмент. Осознанное использование и строгие меры безопасности снижают риски на 85-90%. Безопасность требует постоянной бдительности.

ВЫВОД: МОЖНО ЛИ ДОВЕРЯТЬ СМАРТФОНУ

"Тихий" телефон ≠ безопасный

- 83% троянов невидимы (Kaspersky)

Google Play не защищает

- 23% банковских троянов оттуда (Zimperium)

Обновления критичны

- 60% атак используют исправленные уязвимости

Вы — главная мишень

- 92% заражений через ваши действия

Вывод:

Смартфон — потенциально опасный инструмент. Осознанное использование и строгие меры безопасности снижают риски на 85-90%. Безопасность требует постоянной бдительности.

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЫВОД: МОЖНО ЛИ ДОВЕРЯТЬ СМАРТФОНУ

Основные правила защиты:

Техническая гигиена

- Bluetooth/NFC — только при необходимости
- Только официальные магазины приложений
- Еженедельная проверка разрешений

Финансовая защита

- Отдельный девайс для банкинга
- Аппаратные ключи вместо SMS

«Параноидальные» привычки

- Вручную вводить важные URL
- Нет публичному Wi-Fi для финансовых операций
- Уничтожать чеки/QR-коды после использования

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ
1919

Институт финансовой грамотности – федеральный методический центр повышения финансовой грамотности

IFG@fa.ru