Уникальность – 100% (https://text.ru/antiplagiat/6144566acac3c)

# Как сотрудники могут обманывать системы учета рабочего времени

Точный, строгий и не делающий исключений учет рабочего времени – основа порядка и дисциплины в компании. Если сотрудники знают, что любое опоздание, прогул или другие нарушения рабочего распорядка будут зафиксированы и превратятся в санкции от руководства, они с меньшей вероятностью станут рисковать и делать что-то не так. Поэтому внедрение СУРВ (Системы Учета рабочего Времени) для руководителя – важная задача для любого руководителя.

Классическое решение – организация человеческого контроля. Специально назначенный сотрудник или охранник вручную отмечает в журнале время появления на работе и ухода с нее. Это самый простой, но и наименее эффективный подход из-за человеческого фактора. Намеренные и случайные ошибки с фиксацией времени, «мертвые души», личные договоренности – проконтролировать корректность заполнения табеля крайне сложно.

В общем, ручной контроль нерационален с точки зрения затрат и результата. Но есть целый ряд автоматизированных решений, обеспечивающих более высокую эффективность. Наиболее популярные из них – СКУД, биометрический контроль, трекеры и специальное корпоративное ПО. Ниже мы рассмотрим их, а также наиболее распространенные методики, позволяющие [обмануть системы учета рабочего времени](https://www.kickidler.com/ru/how-to-cheat-time-tracking.html).

## Как обмануть СКУД?

СКУД (Система Контроля и Управления Доступом) – наиболее распространенное сейчас решение среди средств автоматизации. Но не самое эффективное из-за большого количества слабых мест.

СКУД – это магнитные ключ-карты, выдаваемые всем сотрудникам, и считыватели, устанавливаемые на входе в здание или офис. Работник прикладывает карту к устройству, получает доступ в помещение, и одновременно фиксируется время его прибытия на работу.

Преимущество системы – простота. Главный недостаток – СКУД легко обмануть. Например, передав свой ключ сослуживцу, который зафиксирует фантомный выход на работу, что позволит избежать наказания за прогул или опоздание. Еще один вариант – умышленно забыть или потерять карту, из-за чего руководитель будет вынужден вручную вносить данные в отчет, не имея достоверной информации о реальном соблюдении рабочего распорядка.

Кроме того, СКУД – это постоянные расходы для компании, ведь карты теряются и изнашиваются, а терминалы выходят из строя из-за активного использования.

## Как обмануть биометрический контроль по отпечатку пальца?

Контроль с помощью биометрии набирает популярность, поскольку на первый взгляд кажется непогрешимым. Как обмануть биометрию по отпечатку пальца? Ведь только в кино для суперагентов создаются ложные слепки, и происходит это в отлично оборудованных лабораториях. Простому работнику это не по силам!

Известный японский криптограф Цутому Мацумото еще в 2002 году провел исследование и опубликовал [руководство](http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf), позволяющее создать качественный слепок отпечатка пальца в домашних условиях с помощью графитового порошка, суперклея и обычного желе. И его методы оказались действенными – слепки отлично срабатывают.

В 2014 году один из [докладов](https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands) на конференции хакеров Chaos Communication Congress шокировал общественность. Эксперты продемонстрировали настоящий слепок отпечатка пальца министра обороны Германии, созданный на основе качественных фото, взятых из открытых источников. Работоспособность этой технологии подтвердилась и исследованием, проведенным Национального института информатики Японии.

В общем, обмануть биометрику по отпечатку пальца можно. И это даже не слишком сложно.

## Как обмануть биометрический контроль по сканированию лица?

Контроль по биометрии лица кажется еще более совершенным сравнительно с отпечатками пальцев. Но и его можно обойти, причем сразу несколькими методами. Просто обход получится более сложным и дорогостоящим.

Вот только некоторые варианты:

* Как обмануть биометрию радужной оболочки глаза? Оказывается, в большинстве случаев достаточно хорошего фотоаппарата с линзой не менее 200 мм. Как правило, сканеры успешно считывают такие фото.
* Еще один вариант обмана сканера сетчатки – заказать контактные линзы с нужным рисунком радужной оболочки.
* Видеоконтроль можно обмануть с использованием DEEP FAKE. Применение технологий глубокого машинного обучения позволяет создавать видео, демонстрация которых обманывает сканер, заставляя его воспринимать видеоряд как реальность.
* Также контроль по сканированию лица можно обмануть с помощью 3D-маски. Учитывая, что профессиональные фотоаппараты (впрочем, как и 3D-сканеры) и 3D-принтеры редкостью не являются, сделать маску не слишком сложно.

Ненадежность биометрической защиты в 2018 году подтвердили журналисты Forbes, которые [исследовали](https://www.forbes.com/sites/thomasbrewster/2018/12/13/we-broke-into-a-bunch-of-android-phones-with-a-3d-printed-head/?sh=4660dee21330) эффективность распознавания лиц на ТОПовых моделях смартфонов. 3D-маска в 80% помогла разблокировать устройство. Очевидно, комментарии здесь не нужны.

## Как обмануть тайм-трекер?

Тайм-трекер – программа, фиксирующая не только начало и завершение работы за ПК, но и активность сотрудника в течение дня. Это простое ПО, но многие руководители считают его достаточно действенным. На самом деле существуют многочисленные способы обмана тайм-трекера, причем очень доступные:

* Можно запустить любую рабочую программу и приклеить или привязать к мышке любую детскую игрушку, чтобы мышь регулярно двигалась.
* Можно запустить Word, 1C или Excel, минимизировать размеры окна приложения, а дальше включить кино или заниматься чем-то другим, бездельничая.
* Можно купить или написать скрипт или ПО для имитации деятельности, и ничего не делать.

Во всех этих случаях руководитель будет уверен, что сотрудник добросовестно работает, и выявить нарушение удастся разве что случайно.

Работники регулярно придумывают что-то новое для обхода контроля со стороны подобного ПО. Например, интересный [способ обмана тайм-трекера](https://www.kickidler.com/ru/info/obman-ucheta-rabochego-vremeni-ili-kak-odnomu-rabotat-za-pyateryix-klientskij-kejs-12-iz-indii.html) удалось выявить с помощью программы Kickidler. В отделе техподдержки штат из пяти сотрудников. Один из них запускал на своем ПК TeamViewer, подключался через него к остальным терминалам и работал. В итоге трекер регистрировал одинаково высокую активность на всех компьютерах, хотя на рабочем месте находился всего один человек.

## Как обмануть GPS-трекер?

GPS-трекеры работодатели устанавливают преимущественно мерчендайзерам, водителям и другим сотрудникам, работа которых связана с постоянным передвижением и не может быть проконтролирована в офисе. Контроль через спутниковую навигацию на первый взгляд выглядит надежно, но и он не безупречен.

Как обмануть программы для мерчендайзеров с контролем через GPS? Популярные варианты:

* Установка FakeGPS или другого ПО, имитирующего координаты GPS. Можно оставаться дома, а программа будет исправно отсылать данные об активном передвижении.
* Установка на устройство вирусного ПО, что позволяет избавиться от контроля вследствие утраты работоспособности смартфона или планшета.
* Принудительный разряд батареи смартфона – тоже помогает отключить контроль.

В общем, обмануть GPS-трекер тоже не слишком сложно, и для этого не обязательно быть хакером или программистом.

## Как обмануть программу мониторинга сотрудников Kickidler?

Можно смело утверждать, что Kickidler – единственная система учета рабочего времени, которую невозможно обмануть. Причин сразу несколько:

* В отличие от обычных тайм-трекеров и других СУРВ в Kickidler есть функция записи видео с экранов ПК сотрудников. При возникновении подозрений, что работник занимался чем-то другим, можно просто посмотреть, что он делал в интересующее время.
* В Kickidler есть функция просмотра экрана ПК сотрудника в режиме онлайн. Руководитель может в реальном времени посмотреть, занимается ли работник делом, или смотрит кино.
* В Kickidler есть система автоуведомлений «Автокик» для сотрудников, настраиваемых в обширном диапазоне. Система будет сама предупреждать о нарушениях. Например, непрерывная активность в течение 30 минут – это подозрительно, но вручную отслеживать такие аномалии невозможно. А Kickidler способен проводить постоянный мониторинг по любым заданным критериям.

С помощью данного ПО удается раскрывать, как простые, так и хитрые махинации с продуктивностью. Например, функционал системы Kickidler поможет обнаружить [хитрость с зажатой клавишей на клавиатуре](https://www.kickidler.com/ru/info/klientskij-kejs-16-tryuk-s-klaviaturoj-ili-kak-byili-razoblachenyi-kulxaczkeryi.html). Работник запускает Microsoft Word или другую продуктивную программу, ставит на клавиатуру что-то тяжелое, и спокойно смотрит кино в фоне или отдыхает. Любой тайм-трекер расценит такое времяпровождение, как продуктивное. Kickidler же не регистрирует залипание клавиши, как полезное действие. К тому же всегда можно посмотреть онлайн видео с монитора работника.

Также это ПО помогло [обнаружить любителя смотреть сериалы на работе](https://www.kickidler.com/ru/info/klientskij-kejs-15-toss-the-coin-to-kickidler-ili-kak-otvadit-sotrudnikov-smotret-serialyi-v-rabochee-vremya.html). Сотрудник запускал AutoCAD, периодически нажимал на клавиатуру, одновременно смотря в фоне кино. Работодателя насторожило снижение продуктивности, он посмотрел запись с экрана работника и легко выявил нарушение.

Еще один интересный кейс – [обнаружение удаленного сотрудника, занимавшегося фрилансом в рабочее время](https://www.kickidler.com/ru/info/klientskij-kejs-11-xitryij-programmist-ili-kak-byil-pojman-frilanser.html). Подключение к экрану работника позволило установить, что вместо выполнения основной задачи он занимался срочными заказами с фриланс-биржи. И таких примеров того, что Kickidler не обмануть, множество.

Kickidler со 100% точностью регистрирует фактическое начало и завершение рабочего дня, паузы, бездействие и опоздания. Программа предоставляет достоверные данные по учету рабочего времени, и при этом анализирует, как кто работает. Пожалуй, это единственная защищенная СУРВ на данный момент.