ISSN 1815–3305

Кто не спрятался?

Спрос на технологии контроля за персоналом в марте вырос на треть. Бизнес боится утечек и работы «налево».

Российские, и зарубежные разработчики отмечают рост интереса к системам мониторинга персонала. По данным «МегаФона», в марте спрос на решение, позволяющее координировать действия сотрудников с помощью записи разговоров и отчетов о звонках, увеличился на 30%. В «СёрчИнформ» подтверждают: число заявок на бесплатное тестирование выросло на треть. По словам Андрея Коновалова, ведущего эксперта компании Bitcop, спрос вырос больше чем на 30%, в том числе со стороны небольших предприятий. «Малый бизнес очень ограничен в ресурсах, и ему важно использовать их эффективно. Это касается и трудозатрат сотрудников, поэтому работодатель должен знать, чем человек занимается на удаленке», — говорит он.

По оценкам американской Teramind, спрос и вовсе удвоился по сравнению с прошлым годом. У другого международного сервиса, Hubstaff, выручка с конца февраля выросла на 14% и превысила $1,2 млн. «Мы также заметили, что компании, которые уже с нами работали, стали расширять число сотрудников для мониторинга. Если раньше это было плюс–минус пять человек, то теперь 11», — говорит Кортни Кэйфи, директор компании по маркетингу.

Покупка такого софта расценивается как возможность не только контролировать продуктивность работы, но и обезопасить себя. «Многие сотрудники пытаются найти альтернативные источники дохода и в рабочее время могут заниматься чужими задачами — фрилансят, порой работают на прямых конкурентов, — говорит Алексей Дрозд, руководитель отдела информационной безопасности "СёрчИнформ". — Из тех же соображений работники могут продать секреты компании конкурентам или данные клиентов в даркнете». По прогнозам экспертов, количество таких инцидентов в период удаленки вырастет вдвое.

Большой Брат для бизнеса

Как правило, мониторинг персонала осуществляется с помощью отдельной программы, которая устанавливается на компьютер сотрудника. Система предусматривает множество параметров контроля: от учета времени, проведенного за устройством, и анализа используемых ресурсов до записи разговоров и видео с экрана. Например, программа может сообщить, что сотрудник вышел из бизнес–приложения и начал смотреть ролики на YouTube или что он в принципе долго ничего не делал. В организационном плане контроль может осуществляться двумя способами: либо в установленные часы, например с 9 до 18 по будням, либо в зависимости от времени, проведенного в системе. Во втором случае рабочий день сотрудника начинается, когда он зашел в программу, и заканчивается, когда он из нее вышел.

«По обоюдному согласию рабочий день может растягиваться, чтобы у сотрудника был ряд продолжительных "окошек" для решения личных вопросов: приготовить пищу, погулять с собакой или сходить в магазин», — говорит Андрей Арсентьев, руководитель направления аналитики и спецпроектов ГК InfoWatch. Но полностью отключить систему у сотрудника не получится. «Пользователям такой возможности не дается, потому что это сразу привносит соблазн. И даже самые ответственные работники могут ему поддаться. Пользователь может выключить компьютер, но не систему», — говорит Валентин Калаша, руководитель представительства Falcongaze в Петербурге.

С юридической точки зрения удаленный контроль за сотрудниками возможен тогда, когда его применение прописано в локальных нормативных актах и работники с ними ознакомлены. Служащие должны быть в курсе, что за их действиями ведется наблюдение, но оно не должно распространяться на их личную жизнь без веских на то причин. «Российские суды, учитывая соответствующую практику ЕСПЧ, как правило, приходят к выводу, что работодатель не может контролировать личную переписку и собирать сведения о частной жизни работников, если существуют меры, позволяющие достичь той же степени контроля, не затрагивая личную жизнь работника», — говорит Андрей Алексейчук, юрист «Качкин и Партнеры».

Если для работы из дома подчиненный использует технику, принадлежащую компании, то руководитель вправе устанавливать на нее любые программы для мониторинга. Если речь идет о личных устройствах, то это возможно только с согласия сотрудника, а также при условии выплаты ему компенсации. Отказ от использования таких систем может стать поводом для увольнения только в том случае, если их применение закреплено в трудовых обязанностях.

Риск обратного результата

С точки зрения продуктивности тотальный контроль может привести к обратным результатам, когда вместо работы сотрудники будут искать любые способы противодействия системе. «Например, будут писать в тетради, а не печатать на компьютере. Нельзя же к этому придраться? А человек сидит и пишет, как его достал начальник», — говорит Анна Обухова, agile–коуч, партнер компании ScrumTrek.

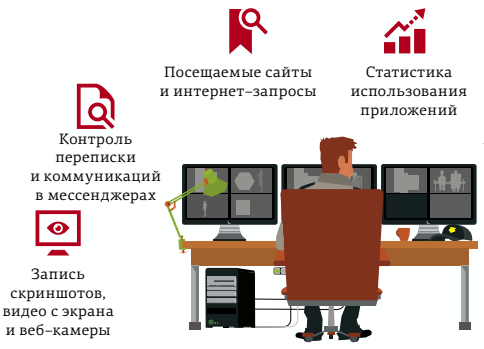
По ее мнению, эффективная работа из дома может быть организована и без систем мониторинга. Для этого руководителям, во–первых, нужно внятно ставить задачи сотрудникам с ориентацией на результат, то есть не «что нужно сделать», а «что должно получиться». Во–вторых, обсудить несколько параметров, включая то, каким должен выглядеть результат конкретной работы, а также критерии приемки — то есть что должно быть сделано, чтобы сказать, что задача выполнена.

«Необходимо составить грамотную систему постановки задач и отчетности, четко продуманную систему коэффициентов эффективности», — согласна Любовь Беляева, психолог, генеральный директор тренингового центра «Фактор Роста».

ЕЛЕНА ВАСИЛЬЕВА
gazeta@dp.ru

ЗА ВАМИ ГЛАЗ ДА ГЛАЗ НУЖЕН

Функционал приложений для слежки



ИСТОЧНИКИ: «МЕГАФОН», FALCONGAZE, HUBSTAFF, INFOWATCH. ИЛЛЮСТРАЦИИ: VOSTOCK–PHOTO. ИНФОГРАФИКА: ФЕДОР ШУМИЛОВ.

МНЕНИЕ

МИХАИЛ ЕМЕЛЬЯННИКОВ
управляющий партнер консалтингового агентства «Емельянников, Попова и партнеры»

Распространение вируса — это удобный повод для внедрения систем слежения. Это все вроде бы объясняется благими намерениями, однако отменить это потом, на мой взгляд, будет практически невозможно. Я считаю, что у нас сейчас есть три модели развития. Одна модель — китайская: с социальным рейтингом, с абсолютно полным пренебрежением правами гражданина и с правом государства делать все, что угодно, что оно считает нужным для достижения цели. Есть модель европейская. В ней возможностей для контроля за гражданами существенно меньше благодаря Общему регламенту по защите данных — GDPR. Основываясь на нем, Евросоюз рекомендовал воздержаться от широкого распространения систем видеонаблюдения с распознаванием лиц ввиду непредсказуемости последствий.

Есть модель США, где, с одной стороны, возможностей для слежки больше, чем в Европе. Этому способствует и принятый после 11 сентября Акт о патриотизме, который ограничивал право на неприкосновенность частной жизни для борьбы с терроризмом, и специальные программы вроде PRISM, о которой в 2013 году рассказал Эдвард Сноуден. Однако, с другой стороны, есть и обратные примеры. Так, в Калифорнии принято решение об ограничении системы распознавания лиц.

Мы пока катимся к китайской модели. Я думаю, что у нас сейчас внедрят различные инструменты контроля и никто даже изменения в закон вносить не будет. Допустим, если в систему видеонаблюдения загрузят безо всякой правовой легализации большое количество фотографий, кто сможет доказать, что они используются, лежат там и так далее? Такой джинн, если его из бутылки выпустили, обратно будет заходить очень неохотно.