Мифы и правда о слежке за компаниями и сотрудниками

Когда разговоры и письма сотрудников компании могут стать доступны налоговой службе, трудовой инспекции и правоохранительным органам. Как подслушивают и подсматривают спецслужбы и есть ли у подозреваемых возможность до официальных обвинений узнать о том, что за ними следят.

Мы собрали частые опасения и предположения о слежке за налогоплательщиками и работодателями и попросили прокомментировать их адвокатов, налоговиков, трудовых инспекторов и специалистов по IT-безопасности, чтобы понять, правда это или миф. Специалисты дали рекомендации, как не допускать утечки информации, и что предпринять, чтобы себя обезопасить.

Легализовать прослушку просто

Чтобы получить разрешение на прослушку нужно всего лишь добавить данные человека или компании в список подозреваемых по какому-либо уголовному делу. Бытует мнение, что судьи на этапе выдачи разрешения обычно не разбираются, как тот или иной контакт связан с материалами дела.

Олег Курандин, адвокат, председатель президиума коллегии адвокатов Пермского края «ПРАВОЗАСТУПНИКЪ», подтверждает, что легализовать прослушку правда не сложно. Но вот использовать полученные записи как доказательство будет сложнее. Оперативники должны убедить судью, что прослушка была обоснована. Подозреваемая компания должна быть связана с фигурантами дела, чтобы суд признал законными доказательства, которые получены в результате слежки.

«Лишь в ряде случаев прослушивание возможно без санкции суда», — замечает Олег Курандин. Но тогда у следственных орга-

нов должна быть достоверная информация о признаках совершаемого или подготавливаемого правонарушения.

МИФ vs ПРАВДА

Правда. Но использовать результаты слежки в суде будет сложно.

У операторов связи стоит специальное оборудование для прослушки всех абонентов

Виталий Балашов, генеральный директор консалтинговой группы «Безопасность бизнеса бэкдор», напоминает, что еще в 1996 году была разработана «Система технических средств для обеспечения функций оперативно-розыскных мероприятий» (СОРМ-1). Она предназначена для того, чтобы проводить расследования в сетях телефонной, беспроводной и радиосвязи. Каждый мобильный оператор на территории России обязан установить эту систему на своих каналах связи.

СОРМ-1 состоит из трех основных частей. Спецслужбы устанавливают у оператора пульт управления, который оплачивает государство. После этого оператор уже за свой счет подключает сервер и прокладывает каналы связи между ним и пультом управления, в том числе VPN. Система позволяет контролировать часть VPN-серверов, прослушивать спутниковую связь, мессенджеры, сохранять данные о совершенных звонках, интернет-сессиях, отправленных сообщениях и выдавать данные из внутренних систем оператора.

Основная задача СОРМ-1 — обеспечивать безопасность государства и его граждан. Поэтому нет смысла слушать всех подряд. Тотальная слежка и прослушивание мобильных телефонов — это лишь страшилки для обывателей. ФСБ выборочно контролирует опасных подозреваемых.

Мероприятия СОРМ осуществляются только по решению суда (Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»). Без него право-

Редакция благодарит за помощь в подготовке статьи:

Наталья Ежова, Советник государственной гражданской службы РФ 3-го класса
Наталья Агуреева, Советник государственной гражданской службы РФ 1-го класса
Олег Курандин, Адвокат, председатель президиума коллегии адвокатов Пермского края «ПРАВОЗАСТУПНИКЪ»
Виталий Балашов, Генеральный директор консалтинговой группы «Безопасность бизнеса бэкдор»
Антон Фишман, Руководитель департамента системных решений компании Group IB
Роман Черненко, Адвокат, руководитель компании «Налоговые адвокаты»

Важно

Как защитить конфиденциальность электронных писем

Перечислю несколько несложных правил, которые помогут вам обезопасить свою переписку.

1. Не заходите в электронную почту на телефоне. Понятно, что это удобно. Однако с конфиденциальной информацией лучше так не делать. В случае потери телефона или его заражения вирусами злоумышленники получат доступ ко всем данным.

2. Используйте специальные сервисы. Они позволяют хранить тексты в зашифрованном виде на отдельном сервере. Чтобы их прочитать, вы должны зайти на этот сервис и ввести свой пароль.

3. Не устанавливайте тот же пароль, что и для других интернет-сервисов. Если пароль будет скомпрометирован на каком-нибудь сайте, то злоумышленники получат доступ и к вашим письмам.

4. Подключите двухфакторную аутентификацию. При каждом входе на почту вы будете получать одноразовый код подтверждения. Таким образом, даже если пароль станет известен третьим лицам, они не смогут зайти в почту.

Антон Фишман, Руководитель департамента системных решений компании Group-IB

Защитить телефон от вирусов
Регулярно обновляйте операционную систему телефона и приложения, устанавливайте только проверенные программы, не рутируйте телефон, чтобы получить доступ к тем приложениям и программам, которые производитель телефона не дает инсталлировать. Внимательно изучите перед установкой, к каким данным хочет получить доступ новое приложение. Чтобы защититься от более сложных вирусных атак, перейдите на SIP-телефонию. Она поддерживает шифрование данных между абонентами.

охранители могут только получить список номеров, с которыми связывался абонент, время звонков и их продолжительность.

МИФ vs ПРАВДА

Правда. Но всех подряд не слушают. Только по решению суда.

Спецслужбы имеют доступ ко всей личной переписке граждан и компаний, так как операторы долго хранят ее

Олег Курандин напоминает, что по новым требованиям «закона Яровой» все интернет-компании, которые входят в реестр организаторов распространения информации на территории Росии, обязаны хранить в течение года сведения об абонентах и фактах приема, передачи, доставки и обработки сообщений и звонков. Шесть месяцев операторы должны сохранять текстовые сообщения, картинки, звуки и видеосообщения (Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»).

Однако для этого необходимо совершить серьезное техническое перевооружение, что под силу не каждому оператору. Провайдеров обязали пока хранить весь проходящий трафик только за один месяц.

Роман Черненко, адвокат, руководитель компании «Налоговые адвокаты» добавляет, что проверку электронной почты спецслужбы могут проводить только на основании решения суда в отношении конкретного гражданина. В отношении неопределенного круга лиц такие действия не проводятся.

Кроме того, на практике такой контроль часто затруднен. Например, доступ к одному компьютеру, адресу электронной почты и пр. могут иметь разные люди. А сами адреса электронной почты могут быть обезличены и не привязаны к конкретному человеку, что лиша-

Важно

Как обезопасить себя от злоумышленников или разведки конкурентов

Ограничьте круг лиц, у которых есть доступ к конфиденциальной информации. Старайтесь не обсуждать ее по телефону. Если вы вынуждены обсуждать с контрагентами свои планы, но не хотите, чтобы о них узнали недобросовестные конкуренты, установите на телефон специальный секретный мессенджер, который можно использовать анонимно и совершать с его помощью полностью зашифрованные голосовые вызовы.

Секретную информацию в электронном виде скопируйте на флеш-карту или жесткий диск и храните вне офиса, но только не дома. Можно рассмотреть хранение информации в облаке. Но нужно быть уверенным в надежности паролей и понимать, как будут действовать владельцы серверов облачных хранилищ, если к ним придет официальный запрос на информацию.

Разработайте положение о коммерческой тайне. Укажите, какая информация не подлежит разглашению и обсуждению, и определите круг доверенных лиц. Также заключите с сотрудниками соглашение о конфиденциальности и внесите соответствующие изменения в трудовой договор.

Если сотрудник нарушит эти положения, ему грозят различные санкции вплоть до увольнения (подп. 6 «в» ч. 1 ст. 81 ТК). В крайних случаях может даже наступать уголовная ответственность (ст. 183 и 272 УК). Обязательно уведомите об этом сотрудников.

Роман Черненко, адвокат, руководитель компании «Налоговые адвокаты»

ет возможности персонализировать электронные сообщения.

МИФ vs ПРАВДА

Правда. Но только по решению суда и в течение месяца после совершения звонка или отправки сообщения.

Запись ведется даже при выключенном телефоне

Телефон может находиться в рабочем режиме, в ожидании и в выключенном состоянии. Легче всего прослушать тогда, когда телефон работает. В режиме ожидания возможно установить только место нахождения телефона, отмечает Олег Курандин.

«Прослушивание выключенного телефона — это фантастика, — считает Антон Фишман, руководитель департамента системных решений компании Group-IB. — Чтобы это реализовать, нужно поставить чип или микрофон внутри аппарата. Это не просто сделать технически и ценность таких действий невелика».

Виталий Балашов добавляет, что если спецслужбы ведут слежку, то они действительно могут активировать микрофон с помощью специальных программ. В этом случае выход один — вытащить из телефона аккумулятор.

Включенный телефон прослушать намного проще. Этим пользуются даже крупные производители смартфонов и владельцы приложений. Именно поэтому Антон Фишман рекомендует при настройке телефона и ПО всегда отключать сбор информации о пользовании устройством и передачу данных производителю.

МИФ vs ПРАВДА

Миф. Но только если вы не находитесь в разработке у следственных органов и они не слушают вас с помощью специальных устройств.

Налоговая может прослушивать разговоры налогоплательщиков

Налоговые органы не имют права самостоятельно проводить оперативно-розыскные мероприятия, включая прослушку разговоров. Но, как замечает Олег Курандин, инспекция может получить у спецслужб результаты расследования в форме справки. При этом она не будет содержать данные о способах, тактике и методике получения информации о подозреваемом (ст. 11 Федерального закона от 12.08.1995 № 144-ФЗ). Порядок предоставления результатов следственных мероприятий закреплен в совместном приказе МВД и ФНС (приказ от 29.05.2017 № 317/ММВ-7-2/481@).

Наталья Ежова, советник государственной гражданской службы РФ 3-го класса, добавляет, что налоговая может получить результаты прослушки только в том случае, если против компании возбуждено уголовное дело и идет совместная выездная проверка со следственными органами. Но даже в такой ситуации следователи могут отказаться передать материалы инспекторам.

МИФ vs ПРАВДА

Миф. Но налоговики могут получать результаты прослушки от спецслужб.

Налоговая имеет доступ к детализации звонков компании

Арбитражный суд в январе 2020 года отклонил иски от МТС, Билайна и Мегафона, которые оспаривали законность штрафа за отказ выдать данные абонентов по запросу налоговой. ФНС доказывала, что детализация звонков поможет проверить правильность налогообложения абонента, а сведения будут «обезличены» и не коснутся тайны переговоров. Инспекция запросила данные о соеди-

Спецслужбы не читают электронную почту у всех подряд

нениях, датах, времени звонков, их продолжительности и стоимости по тому перечню номеров, которые представил сам налогоплательщик.

Инспекторы в ходе выездной налоговой проверки выявили, что записи по телефонным разговорам с одним из контрагентов были задвоены. Чтобы установить обоснованность уменьшения налогооблагаемой прибыли на сумму этих расходов, налоговая и запросила детализацию звонков. Запрошенные данные биллинга не содержали сведений о тайне телефонных переговоров абонентов.

«Сам по себе номер телефона без указания сведений об абоненте является информацией обезличенной, так как набор цифр нельзя признать персональной информацией (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»). Таким образом, ничего страшного в данной ситуации нет. Предприятие должно было лишь обосновать свои затраты на связь», — утверждает Олег Курандин.

МИФ vs ПРАВДА

Правда. Но налоговая не получает доступ к содержанию разговоров.

Трудовая инспекция может прослушивать работодателей

«В трудовом законодательстве не установлен механизм «легализации» записей с прослушивающих устройств или личной переписки работника с работодателем. Законно подслушивать и подсматривать могут только правоохранительные и следственные органы», — комментирует Наталья Агуреева, советник государственной гражданской службы РФ 1-го класса.

Трудовая инспекция может получить материалы уголовного дела, в том числе данные прослушки, только по запросу в следственные органы или суд. Чаще всего инспектор получает обвинительный акт, заключение или приговор суда — это достаточно распространённое явление. Обычно такие запросы связаны с расследованием несчастного случая или, например, при проверках по вопросам невыплаты заработной платы работникам предприятия.

«Были случаи, когда работники предоставляли в ходе проверки записи аудиопереговоров, которые суд ранее уже признал доказательствами вины работодателя. После этого заверенный протокол заседания суда стал доказательством при проверке и рассмотрении административного дела.

Важно помнить, что признание аудиозаписи или переписки доказательством — это компетенция судьи, который выносит решение, руководствуясь законом по своему усмотрению.

В моей практике был случай, когда в рамках одного трудового спора двое судей вынесли разные решения. Истцы в качестве доказательства вины работодателя предоставили письма, которые руководство направляло в адрес сотрудников. Один судья признал их доказательством, а второй — нет.

И произошло это с разницей в полтора месяца», — рассказывает Наталья Агуреева.

МИФ vs ПРАВДА

Миф. Но может использовать решение суда при заведении административного дела.

По некоторым признакам можно понять, что ваш телефон прослушивают

Антон Фишман относится скептически к этому утверждению: «Те признаки прослушки, которые показывают в фильмах, когда в трубке начинает шуршать или идут долгие гудки — бывают только в кино. Если телефон прослушивают силовые ведомства или злоумышленники на уровне оператора связи — человек этого не заметит».

Гораздо более распространённый сценарий — когда аппарат заражен вирусом. Это можно понять по косвенным признакам. Например, стала быстро садиться батарея в новом телефоне, появились уже упомянутые посторонние шумы, зависают приложения и т.д. Но даже эти признаки не однозначны.

Олег Курандин тоже утверждает, что невозможно зафиксировать факт прослушки. Можно только обезопасить себя от последствий. Для этого нужно соблюдать «культуру» общения по телефону и в интернете. «Не болтать» ничего двусмысленного, брать паузу, прежде чем ответить на провокационный вопрос, и помнить, что все сообщения могут в какой-то момент стать публичными.

МИФ vs ПРАВДА

Миф. Это невозможно.