Трудовые споры | 3 Март 2017

ТРУДОВЫЕ СПОРЫ

ТРУДОВОЙ ДОГОВОР

Сотрудник работает за личным ноутбуком. Как обращаться с корпоративной информацией

Ирина Анюхина
партнер юридической фирмы АЛРУД

Марина Юфа
юрист юридической фирмы АЛРУД

1. **Что защитит секреты компании от кражи с ноутбука работника**
2. **Где прописать порядок использования работниками личных устройств**
3. **Платить ли работникам компенсацию за использование личных устройств**

Сейчас многие сотрудники работают с телефонов, планшетов, ноутбуков и проч. Так они могут круглосуточно находиться на связи с начальником, коллегами или общаться с контрагентами из других регионов. Такая концепция получила название Bring Your Own Device (далее — BYOD). Дословный перевод — «принеси свое собственное устройство». Поговорим о том, как внедрить эту концепцию на практике.

Концепция BYOD позволит оперативно связываться с работниками

BYOD — это феномен, который стал возможным благодаря развитию потребительских технологий: их удобству, портативности, мощности, доступности. Как следствие, личные устройства проникли в корпоративную среду. В результате появилось новое поколение работников и новый вид рабочих мест: мобильные и виртуальные.

Исследования показывают, что представители поколения Y отмечают особую ценность возможности использования личных устройств в работе.

Многие компании обращают внимание, что рассматривали внедрение политики BYOD исключительно под напором работников, которые не представляют работу без собственных девайсов.

У инспекторов возникнут вопросы, если работник будет использовать в работе только личные устройства

Преимущества концепции BYOD:

— работник свободен в выборе девайса для общения с начальством и коллегами;

— работодатель может организовать работу в любое время как внутри компании, так и за ее пределами;

— начальник быстрее связывается с работником, а коллеги — друг с другом.

Однако на практике не утихают споры по поводу применения этой концепции. Поднимаются вопросы о несоизмеримости преимуществ концепции и рисков, которые она влечет. Отмечаются и социальные последствия этой новой технологической рабочей реальности. Речь в данном случае идет о круглосуточной доступности работников и влиянии этого на состояние здоровья.

Внимание к концепции привлекают также громкие случаи за рубежом, когда компании дистанционно удаляли всю информацию на личных устройствах, в том числе исключительно личного характера. Делали они это после того, как получали сигналы о возможности кражи информации компании с устройства работника.

Как внедрить концепцию BYOD: пять этапов

В российском праве нет норм, которые регулировали бы порядок внедрения стратегии BYOD. Отсутствуют и разъяснения государственных органов на эту тему. Тем не менее можно выделить ряд мер и принципов, которые позволят внедрить эту концепцию и при отсутствии специального регулирования.

36%

компаний в Северной Америке по данным агентства Gartner используют BYOD

Используйте личные устройства работников как вспомогательные, а не основные средства. По закону работодатель обязан обеспечивать работников оборудованием, которое понадобится для выполнения трудовых обязанностей (ч. 2 ст. 22 ТК РФ). Работник может пожаловаться в трудовую инспекцию, если компания не предоставит ему необходимое оборудование, а укажет на необходимость пользоваться своим.

Чтобы избежать претензий инспекторов, используйте концепцию BYOD в разумных пределах. Например, для определенной категории работников, которые нуждаются в более гибких формах организации трудовой деятельности. Как вариант, в офисе работник пользуется служебным ноутбуком, а когда отходит по делам, то выходит на связь при помощи личного смартфона.

Соблюдайте неприкосновенность частной жизни работников. Концепция BYOD способствует тому, что стирается грань между личным и рабочим временем, а корпоративная информация на устройствах работников соседствует с их личными данными. Неприкосновенность частной жизни не будет нарушена, если вы построите систему защиты информации так, чтобы доступ ИТ-подразделения компании к девайсам работников не затрагивал их личную информацию: приложения, фотографии, мессенджеры, информацию о просматриваемых сайтах и проч.

Также получите у работников согласие на обработку персональных данных на их личных устройствах. Такое согласие должно предусматривать использование устройства работника в служебных целях, мониторинг устройства и право на его использование сотрудниками ИТ-департамента.

Обоснуйте запрет на использование личных устройств для отдельных категорий работников. Компания вправе одним работникам разрешить использовать личные устройства, а другим — запретить. Работники могут заявить, что запрет пользоваться личными устройствами не позволил им повысить эффективность, в отличие от тех, кто имел такую возможность. На такой случай компании важно иметь возможность обосновать цель применения концепции BYOD к определенным работникам.

Также помните, что компания должна предоставить все необходимое оборудование тем сотрудникам, которые не пользуются BYOD, и тем, чьи устройства не соответствуют стандартам, принятым в компании, или по каким-то причинам не позволяют решать их служебные задачи.

Компенсируйте работникам использование личного имущества. По закону работодатель платит работникам денежную компенсацию за использование личного имущества в служебных целях (ст. 188 ТК РФ). Размер компенсации, метод ее расчета и порядок возмещения работодателем с указанием сроков выплаты стороны определяют в трудовом договоре или дополнительном соглашении к нему. Укажите, будете ли выплачивать компенсацию за период отпуска, отгула или больничного.

Также закрепите в договоре:

— наименования личных устройств работника, которые он будет использовать в служебных целях, и их технические характеристики;

— стоимость устройств на дату заключения договора или дополнительного соглашения к нему;

— порядок использования устройств, если он отличается от установленного в локальном акте;

— срок использования устройств.

Обратите внимание, что сумма компенсации относится к расходам на оплату труда. Она не облагается налогом на доходы физических лиц и страховыми взносами, если экономически обоснована и основывается на стоимости используемого имущества работника (абз. 9 п. 3 ст. 217 НК РФ, письмо Минфина России от 18.02.2013 № 03-04-06/4259).

Пропишите в локальном акте порядок использования личных устройств работников. Условия использования работниками личных девайсов в интересах работодателя и другие смежные с ними положения BYOD отразите в положении об использовании личных устройств или ином локальном акте. Не забудьте ознакомить работников под роспись с этим локальным актом.

Корпоративную информацию держите в облачном хранилище, к которому у работника будет доступ с ноутбука

Пропишите следующие положения:

— требования к техническим характеристикам личных устройств и их операционным системам. Это нужно, чтобы обеспечить совместимость этих устройств с другими ИТ-ресурсами компании;

— порядок разграничения корпоративной и личной информации, а также приложений, хранящихся в устройствах. Например, включите положение о запрете доступа работодателя к чатам и мессенджерам;

— положения о мониторинге действий работника, совершенных с использованием личного устройства. Это касается только взаимодействия с ИТ-ресурсами компании;

— порядок установки, использования и обновления антивирусных средств защиты информации, а также шифровальных средств;

— компетенции IT-департамента компании по доступу к устройству;

— порядок действий работников в случае утери или кражи устройства;

— порядок действий при увольнении работника;

— возможность дистанционного удаления данных с устройства в случае инцидента безопасности;

— порядок удаления и (или) блокирования данных в памяти личного устройства.

Многие компании предусматривают в положениях исключительное право IT-департамента устанавливать антивирусные программы и принимать иные решения, призванные защитить информацию. Кроме того, можно установить запрет на использование устройства, не прошедшего процедуру предварительного контроля IT-департаментом.

В целях повышения уровня безопасности компания вправе запретить хранение корпоративной информации непосредственно в памяти устройства работника. Вместо этого можно предоставить работнику доступ к облачному хранилищу данных, снабженному специальной защитой.

Вариант доступа к облачному хранилищу, когда корпоративная информация не хранится на устройстве, исключает разрешение вопроса правомерности удаления данных с личного устройства работника работодателем при инцидентах безопасности.

Инструктаж работников поможет защитить данные компании

Меры обеспечения безопасности персональных данных зависят от угроз безопасности, определяемых самой компанией (оператором персональных данных). Для этого компания привлекает ИТ-специалистов, которые составляют специальный акт — модель угроз.

Угрозы безопасности, в свою очередь, предопределяют соответствующий уровень защиты информационной системы компании, для которого предусмотрен определенный минимальный перечень мер безопасности, закрепленный в законодательстве (постановление Правительства РФ от 01.11.2012 № 1119). Определение угроз безопасности и уровня защищенности — вопросы технического характера.

Но нельзя отрицать, что использование BYOD представляет для компании новые угрозы безопасности. Нейтрализация таких угроз потребует дополнительных мер безопасности и технологических решений. Таким образом, использование в компании стратегии BYOD повлияет на потенциальные угрозы безопасности и применимый перечень мер безопасности.

Многие российские и зарубежные компаний в условиях применения концепции BYOD обучают и инструктируют работников о правилах обращения с устройствами и о том ущербе, который может последовать в случае их кражи или утери.

В данном случае речь идет не просто о формальном ознакомлении под роспись с положением об использовании личных устройств, а о полноценных тренингах и инструктажах с разбором сценариев и порядка действий.

Обратите внимание, что внедрение сервиса BYOD не позволит перенести на работников риски ответственности, связанные с обеспечением конфиденциальности информации, по причине того, что применяемые в ходе работы устройства являются личным имуществом работника и находятся в полном распоряжении последнего. Вся юридическая ответственность за безопасность данных остается на работодателе.

кстати

Главный минус BYOD — риск потери информации компании

Третьи лица могут либо украсть информацию компании с устройства работника, либо украсть само это устройство.

Концепция BYOD находит поддержку все у большего числа работодателей. Экономия, доступность, возможность удаленной работы и круглосуточная связь с работником — все это дает работодателям преимущества в ведении бизнеса. Но обратим внимание и на минусы концепции.

В первую очередь работодателю надо быть предельно внимательным к вопросам информационной безопасности: как к защищенности коммерчески значимой информации, так и персональных данных работников (в том числе работника, использующего личное устройство в интересах работодателя). Помимо этого, при внедрении концепции BYOD работодатель с особой скрупулезностью должен подойти к подготовке положения, регламентирующего использование личных устройств работниками и устанавливающего обязанности работников по обращению с устройствами.

Несмотря на такой привлекательный параметр, как малая ресурсоемкость, работодателю потребуется инструктировать персонал по использованию BYOD. Кроме того, не обойтись без квалифицированного IT-департамента, способного обеспечить информационную безопасность в условиях повышенных угроз. Грамотная регламентация нюансов внедрения и использования сервиса BYOD освободит работодателя от существенных издержек и позволит работникам насладиться преимуществами мобильности.