Корпоративная мобильность: время взять ситуацию под контроль

Текст: **Светлана Пискунова, Екатерина Школина**

Компания ARinteg провела исследование на тему использования сотрудниками собственных мобильных устройств в рабочих целях и безопасности корпоративных данных.

Концепция BYOD (Bring Your Own Device, «принеси свое устройство») активно распространяется среди российских компаний – все больше организаций открывают доступ к корпоративным приложениям через собственные мобильные устройства сотрудников. Исследование, которое провела компания ARinteg, опросив участников мероприятия «Инфофорум-2014», показывает, что большинство компаний разрешает сотрудникам использовать собственные смартфоны и планшеты в рабочих целях, но никак не регламентируют правила их использования (35%). Часть компаний (30%) разрешает сотрудникам использование собственных девайсов при соблюдении определенных условий, руководство ряда компаний не выразило четкой позиции по этому вопросу (21%). В меньшинстве остались респонденты, ответившие, что компания запрещает сотрудникам работать через сторонние девайсы (12%).

Безусловно, удобство и оперативность использования мобильных технологий — это большие плюсы для бизнеса, но эти преимущества «мобилизации» не стоят того, чтобы рисковать безопасностью и репутацией компании.

«BYOD – глобальная растущая тенденция, игнорировать которую руководителям как крупных, так и небольших компаний просто непозволительно, – комментирует Дмитрий Слободенюк, директор компании ARinteg. – Настало время взять ситуацию под контроль, так как неопределенная позиция руководства в отношении использования сотрудниками их собственных устройств может привести к серьезным последствиям».

Преимущества мобилизации бизнеса очевидны, но при ряде плюсов BYOD – таких как оперативность и производительность труда сотрудников, есть и ряд серьезных минусов – прежде всего, это угроза безопасности корпоративных данных.

«Как показали результаты нашего исследования, большая часть руководителей ограничивается лишь рекомендациями по использованию мобильных устройств в рабочих целях – «установите антивирус и будьте бдительны», – добавляет Дмитрий Слободенюк. – Но, полагаться лишь на ответственность сотрудников – большой риск, так как они пользуются девайсами в открытых Wi-Fi сетях, переходят по ссылкам и могут попросту потерять устройство. Все это может привести к потере корпоративных данных. Компаниям необходимо прописать правила использования сотрудниками собственных устройств в рабочих целях и взять на себя вопросы по обеспечению защиты устройств, задействованных в бизнес-процессе».

Сегодня существуют решения, которые позволяют справиться с этой проблемой и организовать безопасный доступ сотрудников с собственных мобильных устройств к сервисам компании. Так, решение для защиты мобильных устройств на примере JC-Mobile от компании «Аладдин Р.Д.» позволяет организовать защищенный доступ к корпоративной почте, корпоративным ресурсам и системам внутри компании, а также обеспечивает юридическую значимость подписываемым электронным документам, письмам, операциям. Таким образом, установив JC-Mobile на свой смартфон, пользователь может безопасно входить в личный кабинет, имея при себе смарт-карту (или Secure MicroSD-токен), проводить и подписывать платежи, будучи уверенным в надежной защите его персональных данных.

«Сотрудники организаций хотят и будут использовать свои собственные устройства на рабочем месте, и закрывать глаза на это явление больше невозможно, – уверен Дмитрий Слободенюк. – Сегодня руководству компаний необходимо всерьез подойти к решению этого вопроса и, обеспечив надежную защиту информации, извлечь из практики BYOD максимум пользы для бизнеса».