Ensuring Information Security in a BYOD-Enabled Organisation
Gavrikov I. (Russian Federation)
Обеспечение информационной безопасности во внедрившей политику BYOD организации
Гавриков И. В. (Российская Федерация)

[1]*Гавриков Илья Владимирович / Gavrikov Ilya – студент,*
кафедра бизнес-информатики и математического моделирования,
Институт экономики и управления,
Крымский федеральный университет, г. Симферополь

Abstract: *the article presents an overview of data and device-related security issues raised by the implementation of a BYOD policy in a corporation and examines some of the possible solutions.*
Аннотация: *в статье рассматриваются проблемы безопасности информации и устройств, связанные с внедрением в корпорации политики BYOD, и изучаются некоторые из возможных решений.*

Keywords: *business, corporate sector, security, information, BYOD, personal devices.*
Ключевые слова: *бизнес, корпоративный сектор, безопасность, информация, BYOD, персональные устройства.*

The unprecedented popularity growth of personal portable devices, such as smartphones and tablets, opens new avenues for corporations, but also raises new issues. The ubiquity of personal devices has resulted in the emergence of the BYOD (bring your own device) philosophy, which aims to increase workforce mobility and cut hardware-related expenses [1]. Experts predict that by 2017, around 50 % of companies worldwide will require their employees to use personal mobile devices for work. Currently, only 22 % of employers consider BYOD to be conducive to business growth, but research shows that by the end of 2016, up to 38 % of companies will use employee devices for work-related purposes [2].

However, this new paradigm is not without its weaknesses, the main of which is corporate data security and personal information confidentiality. Today there are three main security problems associated with the BYOD philosophy, which are the main obstacles on the path to its universal integration:

1) Weak security measures provided by mobile operating systems (iOS, Android), which lack many of the functions required for data security, as well as the means to implement these functions;
2) Full control over BYOD devices by their owners, which significantly limits the degree of control over them and raises the risk of data leaks [3];
3) Lack of a reliable mechanic for separating sensitive corporate data from the personal data of the device owner.

One of the solutions to these problems is using a remote connection between a BYOD device and a secure remote virtual environment protected by a data leak prevention system. This approach has been called vDLP (virtual data leak prevention). An important advantage of this technology lies in the company's full control over the access given to employees and in the secure hosting of sensitive data outside of the BYOD device. A significant drawback of this approach, however, is the need to use virtual environments powered by PC operating systems, which prevents users from utilising their mobile apps of choice for work-related purposes.

An alternative to vDLP that aims to solve its drawbacks is MDM solutions. An MDM (mobile device management) solution is a set of technologies aimed at creating a secure corporate work environment on an employee's personal device. An MDM solution usually includes tools for encrypting sensitive information, as well as tools for remote control over the device and the information it hosts. Thus, this approach preserves the work environment that the user is accustomed to, all the while discretely enhancing it – one of the main requirements for MDM software is minimal influence on the device's and employee's productivity and workflow. This means that an ideal MDM solution integrates into applications used by the user and their work process while protecting any sensitive information from being leaked [4].

The main drawback of the MDM model lies in the difficulty of creating a system that simultaneously satisfies all security and convenience requirements. This is largely due to the high degree of device fragmentation and technical difficulties in implementing security measures due to various limitations imposed by hardware capabilities and company ideologies.

References

1. Insights on the Current State of BYOD. [Электронный ресурс]: Intel IT Center. URL: http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/consumerization-enterprise-byod-peer-research-paper.pdf (дата обращения: 29.05.2016).

2. Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes. [Электронный ресурс]: Gartner. URL: http://www.gartner.com/newsroom/id/2466615 (дата обращения: 29.05.2016).
3. Avoiding BYO Policy and Security Pitfalls. [Электронный ресурс]: Citrix Systems. URL: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/avoiding-byo-policy-and-security-pitfalls.pdf (дата обращения: 29.05.2016).
4. MDM. The solution to BYOD? [Электронный ресурс]: Contextis. URL: http://www.contextis.com/documents/3/BYOD_in_the_Enterprise_-_Context_White_paper.pdf (дата обращения: 29.05.2016).