UDC 004.73

Vitalii A. Savchenko *(Doctor of Technical Sciences, Senior Research Fellow)*

National Defense University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

BRING YOUR OWN DEVICE POLICY AND WI-FI TECHNOLOGY FOR MILITARY EDUCATIONAL ORGANIZATION

This article explores the concept of combining a Bring Your Own Device (BYOD) policy and Wi-Fi technology with existing information policies and infrastructure for typical Military Educational Organization. In face of financial restrictions many Military Educational Organizations in many countries are expecting a problem of computer renewal. To give employees and students an opportunity to work effectively under impossibility to renovate computer facilities a new BYOD policy has to be applied. This policy is directly connected to development of Wi-Fi infrastructure within organization. Obviously, implementing of BYOD policy in a couple with Wi-Fi technology will allow Military Educational Organizations to include into information process not only existent computer hardware, but a great number of personal devices. Nowadays wireless technologies are forbidden for many military organizations because of information restrictions so all aspects of new approach integrity with Net-Centric strategy, efficiency, reliability, security and cost are considered in the article. This article is based on author's experience and represents the author's proposal for the BYOD/Wi-Fi implementation only at the unclassified information environment and the potential financial benefits of this issue.

Keywords: *Bring Your Own Device; Wi-Fi; Military Educational Organization.*

Introduction

In many countries the mass usage of computers in military education started more than 20 years ago. Nowadays for many Military Educational Organizations (MEOs) the problem of computer renewal is very urgent. Many devises were issued many years ago and now became antiquated. Every year MEOs spend lots of money for electronic devises treatment and renovation. Different computer generations use various software that creates a problem of incompatibility. Old computers are mostly desktops that not allow using them easy and flexible. The MEO's local networks, built on Ethernet technologies mostly on twisted pair wiring, do not allow providing fast mobile connection and easy Internet access. Beside of this the usage of personal computing devices and any unauthorized Internet access are forbidden by National security laws and policies because of information security issues.

To solve the problem of effective computer usage in MEO's educational process in face of constant financial restrictions the MEO's authorities should accept and adopt Bring Your Own Device (BYOD) policy [1]. The implementation of this policy in a couple with wireless (Wi-Fi) network development will allow MEO to arise the total number of computers and to provide cost-effective improvement of military education.

Problem Statement. The current mission for the typical MEO is training and professional development of highly qualified specialists for the Armed Forces. In the field of IT it needs development of advanced information technologies into education. The Net-Centric Concept in the sphere of military education needs us to be joined to the Global Educational Environment (information resources, databases, scientific sites etc.) and to develop the Distant Learning systems. The Global Educational Environment can help students to be "in touch" with latest tendencies in the sphere of defense providing the most actual approaches in military management as well as foreign experience in modern warfare. The Distant Learning can help educators to bring all actual information to students via information means wherever they are.

Nowadays we spend lots of money for new hard and software, for maintenance and renovation of existent equipment. Financial limitations face us with dilemma how to manage our resources effectively. And, in the same time, the park of personally owned devises (laptops, tablets, smartphones) grows fast. But for this moment wireless technologies are limited in usage in many military educational organizations.

So, the problem of MEO's computer infrastructure development goes to the forward plan. Implementation of BYOD policy in a couple with development of Wi-Fi infrastructure in MEO's unclassified domains potentially can solve this problem and save money. All of this will help MEOs to arise the quality of military education and that's why the questions of BYOD/Wi-Fi implementing as well as problems of policy adaptation, security and cost-benefit analysis have to be considered in detail.

BYOD/Wi-Fi an Emerging Approach

BYOD policy. *Bring your own device* is a policy that implies of permitting employees to bring personally owned mobile devices to their workplace and to use those devices to access company's information and applications [1].

The term BYOD was first introduced in 2009 when Chief Information Officers (CIOs) in IT companies were really starting to feel the pressure as personal devices flooded the workplace. In 2012 IT experienced the first real concerns around BYOD security and data leakage. On the other side, users were becoming increasingly concerned about their

privacy. Since 2013 innovations in data security, such as email, apps, and content containerization, have become popular. This containerization helped to separate personal data from corporate data. Since 2014 BYOD has slowly being morphing into *Bring Your Own Everything* (BYOx): device, apps, encryption, identity, technology, network, wearable etc. [2, 3]. But, despite of all, BYOD still remain the center of all of this approaches so the topic of this work will be restricted within BYOD policy.

For military applications BYOD mostly is still a new undiscovered idea. During 2012 – 2013 US Department of Defense (DoD) many times looked on this idea but every time the question was delayed due to information assurance issues [4, 5]. Now the US DoD also is getting ready to launch a pilot program to examine the viability of a BYOD within the military. Most likely, potential BYOD privileges would be limited to certain users and certain types of use, such as e-mail access, file-sharing and calendar applications on certain approved personal devices [6].

Despite of Pentagon's doubts about BYOD in military headquarters (HQ) and combat units some US military organizations, where cost of information is not "so high", have effectively realized this policy. So, the US National Defense University (US NDU) is a BYOD campus. Students are free to bring a privately-owned (recommended for ease of configuration) computing devices capable of Wi-Fi connectivity. At the same time US NDU's IT Directorate highly discourages the use of government-owned devices on its Wi-Fi network [7].

The important issue with BYOD is of scalability and capability. Many MEOs today lack proper network infrastructure to handle the large traffic which will be generated when employees will start using different devices at the same time, that increases demands for Wireless Local Area Network (WLAN) infrastructure development [1].

Drawing the bottom line of BYOD consideration it's possible to make some conclusions in a view of future implementation of this policy into a MEO. *Positive*: (1) Ability of today's users to work anywhere on any device: in a classroom or at home. (2) Ability of today's organizations to create more comfortable environment for their employees and to decrease financial spending on information facilities and infrastructure. (3) Full realization of the Net-Centric Concept via involvement of personnel and their equipment into the current educational process anywhere and anytime.

Negative: (1) Security – MEO's data is vulnerable to illegitimate access. Any number of users could have an infected email client or malware apps could be injected into the network. (2) Privacy – the network has to separate people's private data from MEO's data. (3) Data integrity – data is not sat on the server but it's sitting on mobile devices [8].

Wi-Fi technology. According to **[9] Wi-Fi** is a local area wireless technology that allows an electronic device to participate in computer networking using 2.4 GHz UHF and 5 GHz SHF ISM radio bands. The Wi-Fi Alliance, that was formed in 1999 as a non-profit association to hold the Wi-Fi trademark, defines Wi-Fi as any WLAN product based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards. The 802.11 protocol was released first in 1997 and provided up to 2 Mbit/s link speed.

The Wi-Fi signal **range** depends on the frequency band, radio power output, antenna gain and type. An Access Point compliant with either 802.11b or 802.11g, using the stock antenna might have an open range of 100 m (330 ft). The same radio with an external semiparabolic antenna (15db gain) might have a range over 20 miles [9].

The **speed** of data transmitting depends on environment and applied protocol. It varies from 1 – 2 Mbit/s for 802.11a up to 6.75 Gbit/s for 802.11ad. Full description of technical parameters of IEEE 802.11 protocols are given in [10].

Nowadays Wi-Fi technology is often used to provide Internet access to devices that are within the range of a WLAN that is connected to the Internet. The coverage of one or more interconnected access points (hotspots) can extend from an area as small as a few rooms to as large as many square kilometres. Coverage in the larger area may require a group of access points with overlapping coverage [9]. Now many universities deploy Wi-Fi infrastructure in their campuses. At MEO Wi-Fi can be used for local indoor networks deployment (see Fig. 1) as well as for wide outdoor applications. This article considers only indoor Wi-Fi applications for MEO. Exploring possibilities to improve information infrastructure in MEO it's necessary to consider Wi-Fi advantages and disadvantages.

Wi-Fi Advantages: (1) *Cost*. Wi-Fi allows cheaper deployment of WLAN including spaces where cables cannot be run (using MESH topology). In face of financial restrictions this Wi-Fi feature can be a keystone for future decision. (2) *Convenience*. The wireless nature of Wi-Fi networks allows users to access network resources from nearly any convenient location within MEO. (3) *Security*. Wi-Fi networks can be adequately protected by enabling password protection and data encryption. A Wi-Fi network using WPA2 provides both security (you can control who connects) and privacy (the transmissions cannot be read by others) for communications. All of this gives MEO customers the ability to work with information safely.

Wi-Fi Disadvantages: (1) *Security*. Despite of all modern approaches security still remain the week point of Wi-Fi. Potentially, unauthorized users can be connected to Wi-Fi network. So, wireless networks have to utilize various encryption technologies available. (2) *Range*. The typical range of a common 802.11g network with standard equipment is on the order of 45m (150ft) indoors. To obtain additional range, repeaters or additional access points have to be purchased that considerably increases the network cost. (3) *Speed.* A public Wi-Fi network is very dependent of the number of users. The speed on most wireless networks (typically 1 – 54 Mbps) is far slower than even the slowest common wired networks (100Mbps up to several Gbps). However, the new

generation of IEEE 802.11 protocols promises to solve this problem.

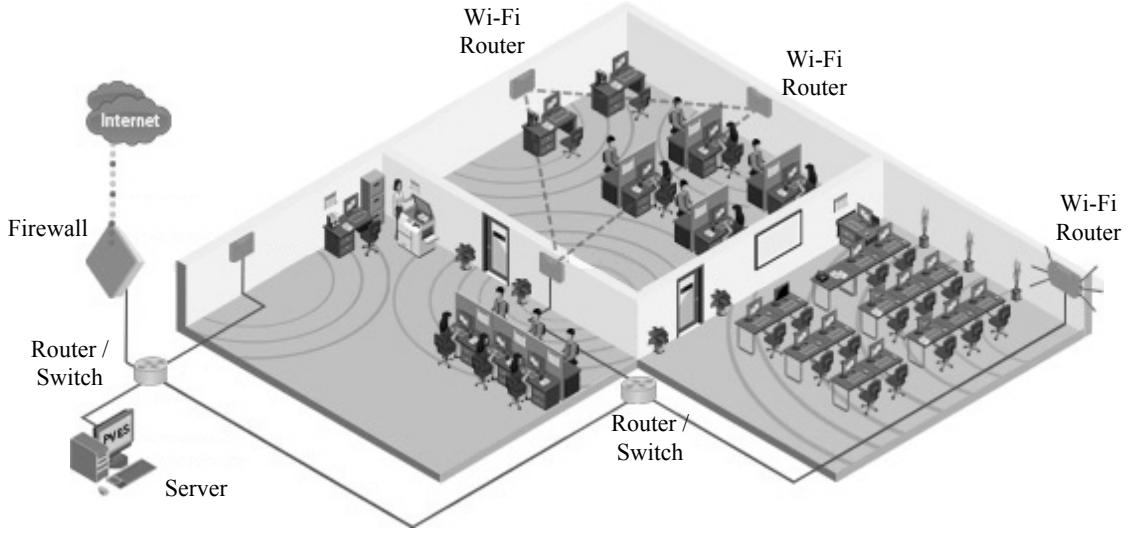

Figure 1. An example of WLAN in an office environment [11]

Laws and Policy

In many countries the main directions of IT implementation into education are declared by the National Telecommunication Legislation that imply creation of fully informatized campuses within schools and universities. But in military sphere these Laws are some limited by the National Information Security Legislation that limit personal mobile devises application and wireless networks deployment in organizations where people can be connected to the National or military secrets. MEO educates students of strategic, operational and tactical level so potentially they are connected to those secrets.

So the contradiction appears: from one side MEOs need to join to the world resources and have to implement BYOD/Wi-Fi and, from the other side, they have to cut down any IT that can potentially compromise existed classified information.

By author's opinion all limitations can be explained only by higher authorities' "misunderstanding" of role and capabilities of new technologies. More careful learning of Laws and Orders drives us to conclusion that the main idea of information security in technical sphere is not to allow restricted and unrestricted devises working together. This conclusion drives to a decision – to separate (physically and technically) restricted and unrestricted information environments. So, the special separated zone has to be created on the territory of MEO for work with classified information. It has to be free of any wireless technologies and be out of BYOD policy. This decision can be confirmed by analysis of student's educational process: only some percent of total students information is classified and the total square ratio of restricted territory has to be the same.

This short research shows that generally National Legislation allows MEO to implement BYOD/Wi-Fi, but they should make appropriate changes in some documents on local level. These changes have to be directed onto separation information environments and creation of secure unclassified information infrastructure.

Efficiency

Efficiency of BYOD/Wi-Fi for MEO can be measured by potentially gained educational effectiveness that depends on: staff productivity, employee satisfaction etc. BYOD/Wi-Fi is quite new strategy for military education so there are no real researches over these issues but its predicted efficiency can be approximately estimated on the basement of other researches. The research conducted by Willis [12] in Europe, the Middle East and Africa shows employer's estimations of current BYOD programs (see Fig. 2).

Cost Benefit Analysis

Detailed research for BYO efficiency also was made by Troni and Silver [13]. This research shows that BYOD policy can be very financially effective mostly in its "clean" variant, when employees use their equipment not demanding reimbursements and minimizing any other spending on their own devices. For example (see Fig. 3) in case of tablets use of User-owned (semimanaged) items gives an effect up to 64% comparing with Enterprise-owned tablets fully-managed. But, if tablets use additional services such as server-based computing (SBC) or hosted virtual desktop (HVD) technologies, the total cost of ownership (TCO) increases, in some cases substantially [13].

The current necessary MEO spending for existent infrastructure development consists of costs for: computer purchasing, LAN development (equipment and its deployment), software licensing, maintenance of existent MEO's computers, computer renovation.

The total financial efficiency of BYOD/Wi-Fi for typical MEO can be described by the next artificial example. Having 2,000 computers for 2,500 MEO's people (employees and students) to supply users by computers we have additionally to purchase 500 computers. Also, lets for further infrastructure development we need 20 switches and 4,000 m of wired cable. Basing on prices [14] it will cost: computers Dell Inspiron (500 × $500 = $250,000): switches D-Link DGS (20 × $250 = $5,000); wired cable (4,000m × $0.2 = $800); deployment works $1000.

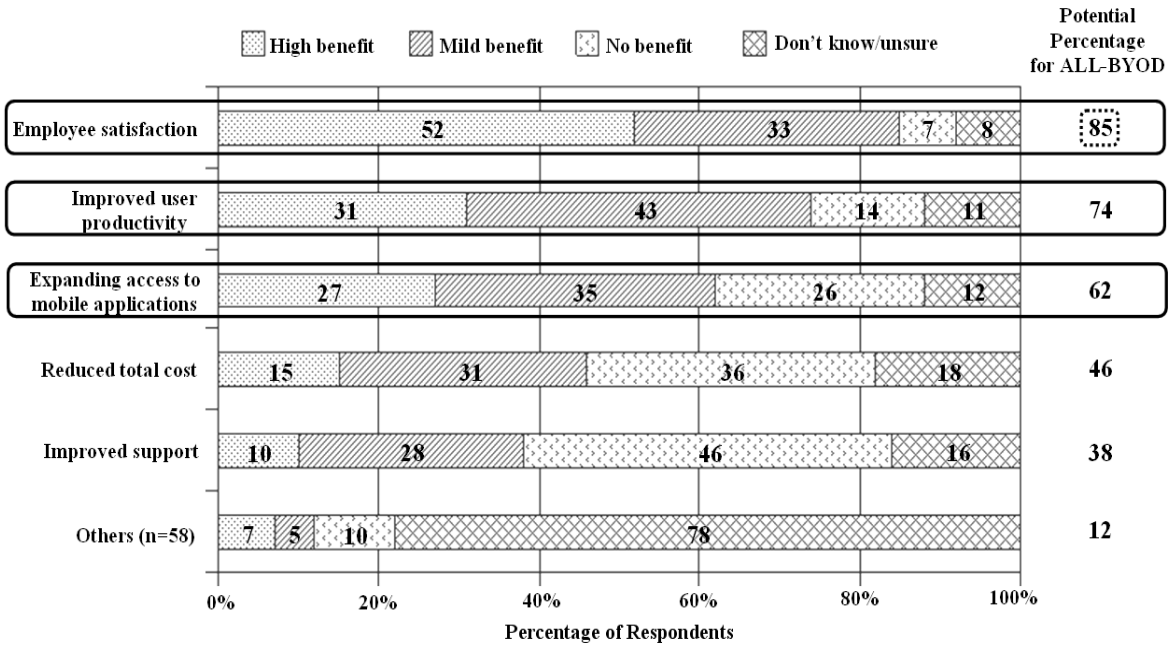

Figure 2. Benefits Realized From Current BYOD Program [12]

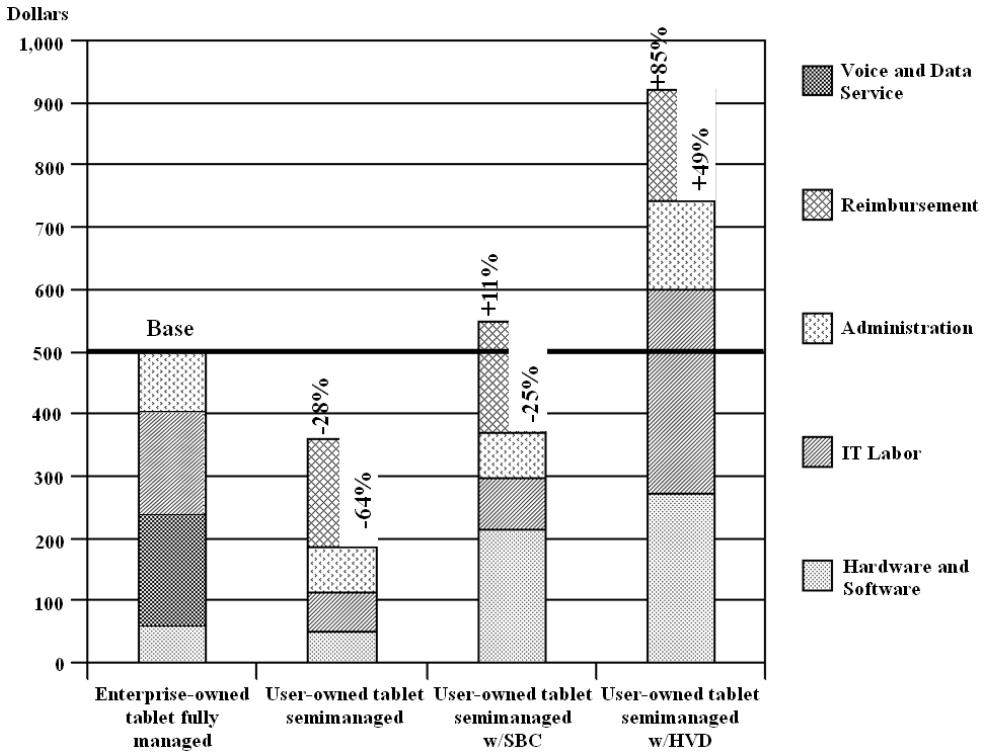

Figure 3. TCO Comparison of Enterprise- and User-Owned Tablets [12]

For new computers we have to purchase licenses for operating systems (Win7 - $82), office programs (MS Office 2010 - $180) and antivirus (Norton - $35), that totally will cost: 500 × ($82 + $180 + $35) = $148,500. Maintenance of existent MEO's computers can be approximately accounted on the basement of the price of 1 comp. maintenance per year: 2,500 × $20 = $50,000. Computer renovation implies that 20% of all computers in a year have to be replaced by new ones: 400 × ($500 + $295) = $318,000. So, according to the Net-Centric Concept and the main goal to be joined to the Global Educational Environment the total necessary MEO spending for existent infrastructure development during the next year has to be: $250,000 + $5,000 + $800 + $1000 + $148,500 + $50,000 + $318,000 = **$773,300**.

Probable MEO spending for WLAN infrastructure development and BYOD implementation in its "clean" variant will consist only of Wi-Fi network development (equipment and its deployment) and spending for restricted and unrestricted zones separation. Basing on prices [14] it will cost: routers

D-Link DSR-500 (8 × $300 = $2,400); wired cable (1,500m × $0.2 = $300); Wi-Fi routers Cisco SB RV220W (20 × $350 = $7,000); deployment works $1200. Existent computers maintenance per year (50% of existent computers will be used despite of BYOD concept): 1,000 × $20 = $20,000. So, to reach the main goal of MEO the total necessary spending for BYOD/Wi-Fi concept and existent infrastructure maintenance during the next year has to be: $2,400 + $300 + $7,000 + $20,000 = $29,700. Restricted/unrestricted zones separation will consist of payments for student classes movement ($100,000) and their certification ($50,000), totally – $150,000. So, the total necessary spending for BYOD/Wi-Fi policy implementation will be $29,700 + $150,000 = **$179,700**.

As we can see the cost benefit for BYOD/Wi-Fi (in a year prospective) is $773,300 – $179,700 = **$593,600**. So, we need less than a year to see cost benefit of BYOD/Wi-Fi. In the most difficult case, if we are not able to renovate existent and to buy new computers and need to spend money only to their maintenance: 2,000 × $20 = **$40,000** per year; in this case the **Response Time** for BYOD/Wi-Fi policy will be $179,700 / $40,000 = **4.5 years**.

But, according to Willis [12], cost reduction is not universally achievable with BYOD. Many organizations say that they spend more money after implementation of BYOD but even though the savings potential is lackluster, organizations often see other benefits, which are driving investments in BYOD.

Security Issues

Problems with BYOD security are connected with the End Node Problem [15] that causes some risks: a) employee can lose the device and untrusted parties could retrieve any unsecured data; b) employee can leave the company but company applications and other data may still be present on its device [1].

Mostly BYOD/Wi-Fi, as s new strategy, doesn't have any analogs in Armed Forces so these issues should be considered on the basement of world's best practice separately for both of components: BYOD and Wi-Fi.

On the basement of BYOD research results, highlighted in [16], MEO Staff should: (1) *Set standards* for users by establishing an acceptable-use policy. (2) *Identification* for BYOD is critical. All users (individuals, groups and devices) have to be identified. IT administrators have to establish restrictions and allowances, such as applications and content for individuals, groups and types of devices. (3) *Enforcement***.** It's necessary to have employees' signatures as acknowledgement of the rules and their required compliance to participate in the program. (4) *Execute***.** It's critical to choose a platform that is agile and scalable enough to not only keep up with user demands and protect corporate assets, but also accommodate emerging technologies as well. (5) *Help***.** By providing support, MEO IT can help employees manage devices and access controls, discover potential vulnerabilities and further enforce BYOD policies.

Wi-Fi security issues are based on the vulnerable wireless nature and growing crime cyber activity. The technical and social aspects should be reflected in MEO's Security Policy that, beside of others, should include [17]: (1) *Register Access Points*. All wireless Access Points / Base Stations connected to the network must be registered and approved by MEO. (2) *Approved Technology*. All WLAN hardware implementations shall utilize Wi-Fi certified devices that are configured to use the latest security features available. (3) *Physical Location*. Security mechanisms should be put in place to prevent the theft, alteration, or misuse of Access Points / Base Stations. (4) *Configuration*. The default SSID and administrative username / password shall be changed on all Access Points / Base Stations. Device management shall utilize secure protocols such as HTTPS and SSH. Access Points / Base Stations should be placed strategically and configured so that the SSID broadcast range does not exceed the physical perimeter of the building/territory. Console access shall be password protected. (5) *Authentication and Transmission*. All wireless access points that connect clients to the internal network (LAN) shall require users to provide unique authentication over secure channels and all data transmitted shall be encrypted with an approved encryption technology. (6) *Internet-only Deployments*. Access Points / Base Stations deployed to provide Internet-only service shall be separated from the internal network by denying all internal services. (7) *Enforcement*. Any employee found to have violated the policy may be subject to disciplinary action up to and including termination of employment.

Following these recommendations MEO will minimize risks of inappropriate information flow and will make convenient environment for Staff and students.

Implementation Strategy

BYOD/Wi-Fi Implementation Strategy should be based on gradual Wi-Fi equipment deployment following after the initial project approved by Information Security Office. After adoption of all necessary legislative issues for deployment of BYOD/Wi-Fi policy the Staff of MEO have to create a Management Policy.

In [18] the BYOD Deployment Guideline is given. The key point of this Guideline is a Plan for Implementing a BYOD Solution. For good planning an understanding of the current Wi-Fi capacity and coverage is critical. Also Provisioning Infrastructure and Devices as well as Proactively Manage and Troubleshoot have to be the part of BYOD/Wi-Fi Implementation Strategy. Describing BYOD implementation strategy Horwath [19] distinguishes the necessity of specialized group creating: Initiating, Planning, Executive and Monitoring. The task of these groups is to perform projects and plans as well as to control their implementation.

The process of BYOD/Wi-Fi Implementation at MEO should consist of the next steps: (1) Territorial and technical separation of restricted/unrestricted information environment; (2) Wi-Fi infrastructure deployment; (3) Wi-Fi system testing and certification; (4) User and personal devises registration and identification.

Support of Net-Centricity

Net-centric refers to participating as a part of a continuously-evolving, complex community of people, devices, information and services interconnected by a communications network to achieve optimal benefit of resources and better synchronization of events and their consequences [20].

For the most of MEOs integration and cooperation with other universities/colleges is a part of MEO's vision, so their educational environment has to be connected to the World common educational environment that means data exchange, common E-learning etc. Truyen & Van Rentergem [21] establish Net-Centric approach for educational organization as: "highly layered infrastructure that is bound together with open standard protocols, which enable a modular design of the support resources throughout the university and associated networks" [21, p. 12].

The key factors in this case are the large databases used for MEO's educational process: audio-visual material, course materials, courses, course descriptions, dissertations, other data.

Consequence of Adaptation on Policy

BYOD/Wi-Fi Policy should describe all aspects of MEO's information security but has to be directed to creation of real productive infrastructure. Implementing this policy MEOs can get many advantages that bring them into the world educational level. Avoiding BYOD/Wi-Fi means serious delay for MEO in the quality of education and considerable financial spending for existent infrastructure.

No one new technology comes without risks and vulnerabilities. The most of BYOD/Wi-Fi technical vulnerabilities and risks are connected to Wi-Fi technology but the following use of Wi-Fi networks that threatens data and network security should be banned under most circumstances [22]: (1) Rogue Access Points (AP) – Unauthorized installation of APs poses a threat to information security; (2) Ad hoc mode – This peer-to-peer mode of Wi-Fi networks actually converts the computers/workstations involved into rogue APs, because any workstation is equivalent to an AP under this mode.

To avoid consequences of BYOD/Wi-Fi policy violation MEO has to reserve the right to disconnect employee's devices or disable services without notification and to take appropriate disciplinary action for noncompliance with BYOD/Wi-Fi policy.

Conclusion

In face of financial problems for many countries the Bring Your Own Device policy is a good solution for the problem of computer usage in military education. The implementation of this policy in a couple with Wi-Fi network development will allow MEO: to realize the Net-Centric educational strategy, to arise the total number of computers that can be involved into educational process, to get employee's satisfaction and to attract new students. All of this allows providing cost-effective improvement of military education.

Effective implementation of BYOD/Wi-Fi policy at MEO needs to change some legislation on the base of territorial and technical separation of restricted/unrestricted information environment. Some potential risks of BYOD/Wi-Fi implementation can be minimized by all participants' strict precision of information security rules and prescriptions given in Security Policy. Experience, gained from some world MEOs, particularly The National Defense University of the USA, just can confirm the key issues of this article.

In future BYOD/Wi-Fi policy at MEO opens wide possibilities for further IT innovations such as cloud computing, big data store etc.

References

1. Bring your own device. (2015). Retrieved February 01, 2015, from Wikipedia: https://en.wikipedia.org/wiki/Bring_your_own_device#cite_note-10. **2. Laird J.** (2014, November 07). A Brief History of BYOD and Why it Doesn't Actually Exist Anymore. Retrieved February 01, 2015, from Lifehacker.uk: http://www.lifehacker.co.uk/2014/11/07/brief-history-byod-doesnt-actually-exist-anymore. **3. Rouse M.** Bring your own everything (BYOx) (2014, April). Retrieved February 01, 2015, from TechTarget: http://searchconsumerization.techtarget. com/definition/bring-your-own-everything-BYOx. **4. Perera D.** BYOD for unclassified at DoD possible in 2014. (2012, July 22). Retrieved February 01, 2015, from Fierce GovernmentIT: http://www.fiercegovernmentit.com/story/byod-unclassified-dod-possible-2014/2012-07-22. **5. Hickey K.** DOD plan for mobile not BYOD-ready. (2013, March 01). Retrieved February 01, 2015, from Government IT Outcomes Resource Center: http://gcn.com/articles/2013/03/01/dod-plan-for-mobile-not-byod-ready.aspx. **6. Corrin A.** DoD Pursuing Options for BYOD, SIPRNet mobility. (2014, October 02). Retrieved February 01, 2015, from FederalTimes: http://archive.federaltimes.com/article/20141002/mob/310020026/dod-pursuing-options-byod-siprnet-mobility. **7. Information** Resources Management College. Bring Your Own Device. (2015). Retrieved February 02, 2015, from iCollege official site: http://icollege.MEO.edu/Students/BringYourOwnDevice.aspx. **8. Harris M.** What's in Your BYOD World? Biometrics is key to network-centric security. (2013, May 01). Retrieved February 02, 2015, from SecurityToday: http://security-today.com/articles/2013/05/01/whats-in-your-byod-world.aspx. **9. Wi-Fi.** (2015). Retrieved February 02, 2015, from Wikipedia: http://en.wikipedia.org/wiki/Wi-Fi. 10. IEEE 802.11. (2015). Retrieved February 02, 2015, from Wikipedia: http://en.wikipedia.org/wiki/Wi-Fi. **11. An Introduction** to 2.4GHz Technology. (2015). Retrieved February 05, 2015, from 4Gon: http://www.4gon.co.uk/solutions/introduction_to_2_4ghz.php. **12. Willis D.A.** Bring Your Own Device: The Results and the Future. (2014, May 05). Retrieved February 03, 2015, from Gartner: http://www.gartner.com/document/2730217?ref=QuickSearch&sthkw=byod%20efficiency&refval=147131092&qid=10808cac46b21fbc578e2541ea969157. **13. Troni F.,** Silver M.A. Understand the Financial Impacts of BYOD. (2014, December 04). Retrieved February 02, 2015, from Gartner: http://www.gartner.com/document/2935917?ref=QuickSearch&sthkw=byod&refval=147083479&qid=dd307bb5fecfc9c8759a04aa1ff5b1b9. **14. Internet** shop Rozetka (2015). Retrieved February 10, 2015, from Rozetka.com: http://rozetka.com.ua. **15. End** node problem.

(2015). Retrieved February 01, 2015, from Wikipedia: https://en.wikipedia.org/wiki/End_node_problem. **16. Angeles S.** BYOD Security: 5 Risk Prevention Strategies. (2014, August 06). Retrieved February 04, 2015, from BusinessNewsDaily: http://www.businessnewsdaily.com/6924-byod-security-policy.html. **17. Wireless** LAN Security Policy. State of Maryland. The Department of Information Technology. (2014). Retrieved February 04, 2015, from DoIt: http://doit.maryland.gov/support/Documents/security_guidelines/DoITWirelessCommunicationPolicy.pdf. **18. BYOD** Best Practices. Requirements and Challenges. (2013). Retrieved February 04, 2015, from MeruNetworks: http://www.merunetworks.com/collateral/white-papers/wp-byod-implementation-whitepaper-for-wlan-security.pdf. **19. Horwath J.** Managing the Implementation of a BYOD Policy. GIAC (GCPM) Gold Certification. (2013). Retrieved February 04, 2015, from SANS Institute InfoSec Reading Room: http://www.sans.org/reading-room/whitepapers/leadership/ managing-implementation-byod-policy-34217. **20. Net-centric** (2015). Retrieved February 05, 2015, from Wikipedia: http://en.wikipedia.org/wiki/Net-centric. **21. Truyen F.,** Van Rentergem L., Preparing the University Information Architecture for Net-centric E-learning and Research: a case-study. (2006). Retrieved February 05, 2015, from Leuven: http://www.virtualschoolsandcolleges.eu/images/0/0f/EQIBELT_KULeuven_Truyen_paper.pdf. **22. Du H.,** Zhang, C. Risks and Risk Control of Wi-Fi Network Systems. (2006). Retrieved February 05, 2015, from Information Systems Control Journal: http://www.isaca.org/Journal/Past-Issues/2006/Volume-4/Documents/jpdf0604-risks-and-risk-control.pdf.

ПОЛІТИКА “ПРИНЕСИ СВІЙ ПРИЛАД” ТА WI-FI ТЕХНОЛОГІЯ ДЛЯ ВІЙСЬКОВОГО НАВЧАЛЬНОГО ЗАКЛАДУ

Віталій Анатолійович Савченко *(д-р техн. наук, с.н.с.)*

Національний університет оборони України імені Івана Черняховського, Київ, Україна

У статті досліджується концепція поєднання політики “Принеси свій прилад” та Wi-Fi технології з існуючою інформаційною політикою та інфраструктурою типового військового навчального закладу. В умовах фінансових обмежень багато військових навчальних закладів в багатьох країнах зіштовхнулися з проблемою оновлення комп’ютерної техніки. Для того щоб надати працівникам та слухачам (курсантам) можливість ефективно працювати в умовах неможливості оновлення комп’ютерної техніки повинна бути прийнята нова політика “Принеси свій прилад”. Ця політика безпосередньо пов’язана з розвитком Wi-Fi інфраструктури організації. Очевидно, що впровадження цієї політики разом з Wi-Fi технологією дозволить військовому навчальному закладу долучити до інформаційного процесу не лише існуюче комп’ютерне обладнання, але й значну кількість особистих засобів. На сьогоднішній день використання безпроводових технологій у багатьох військових організаціях заборонено через заходи інформаційної безпеки тому у статті розглянуто переваги нового підходу з точки зору мережецентричності, ефективності, надійності, безпеки та вартості. Стаття базується на досвіді автора та відображає його пропозиції виключно для нетаємного інформаційного середовища а також пов’язані з цим потенційні фінансові переваги.

Ключові слова: *Політика “Принеси свій прилад”; Wi-Fi; військовий навчальний заклад.*

ПОЛИТИКА “ПРИНЕСИ СВОЙ ПРИБОР” И WI-FI ТЕХНОЛОГИЯ ДЛЯ ВОЕННОГО УЧЕБНОГО ЗАВЕДЕНИЯ

Виталий Анатольевич Савченко *(д-р техн. наук, с.н.с.)*

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье исследуется концепция интеграции политики “Принеси свой прибор” и Wi-Fi технологии с существующей информационной политикой и инфраструктурой типового военного учебного заведения. В условиях финансовых ограничений многие военные учебные заведения во многих странах столкнулись с проблемой обновления компьютерной техники. Для того чтобы предоставить персоналу и слушателям (курсантам) возможность эффективно работать в условиях невозможности обновления компьютерной техники должна быть принята новая политика “Принеси свой прибор”. Эта политика непосредственно связана с развитием Wi-Fi інфраструктури организации. Очевидно, что внедрение этой политики вместе с Wi-Fi технологией позволит военному учебному заведению привлечь к информационному процессу не только существующее компьютерное оборудование, но и значительное количество личных средств. На сегодняшний день использование беспроводных технологий во многих военных организациях ограничено из-за требований по информационной безопасности поэтому в статье рассмотрены преимущества нового подхода с точки зрения сетецентричности, эффективности, надежности, безопасности и стоимости. Статья базируется на опыте автора и отображает его предложения исключительно для несекретного информационного пространства а также связанные с этим потенциальные финансовые выгоды.

Ключевые слова: *Политика “Принеси свой прибор”; Wi-Fi; военное учебное заведение.*

Отримано: 21.05.2015 р.