American Journal of Science and Learning for Development

Volume 1 | No 2 | Dec-2022

Use of Personal Mobile Devices in Higher Military Education Schools

Sapaev Jasurbek Kamilovich [1], Uralov Xusan Boboqulovich [2]

[1] *National University of Uzbekistan named after Mirzo Ulugbek, Head of the scientific department of the military training center, major in the reserve*

[2] *National University of Uzbekistan named after Mirzo Ulugbek, Senior teacher of the cycle of chemical protection and topogeodetic supply of the Military Training Center of the Engineer-Sapyar troops, associate professor, lieutenant colonel in the reserve*

Abstract: *A variety of personal mobile devices have firmly entered the life of modern man and society. However, the threats associated with them forced the law enforcement agencies to prohibit not only the use, but also the presence of these devices on the territory of special-purpose facilities. In turn, the capabilities of these devices, subject to the creation of the proposed model for building and managing the information security system of a special purpose object, can be used to effectively solve a number of urgent problems.*

Keywords: *personal mobile devices, smartphone, tablet, laptop, smart clock, fitness bracelet, higher military educational institutions, Bellingsat, information security, monitoring, armed conflicts, infocommunication, Geo-location, antivirus, brandmauer, WiFi Wireless Network, Internet, threats.*

In the conditions where globalization continues and the entire system of international relations is changing, the military-political situation in the world is increasing the scope of dangers and threats to international and regional security - the intensification of geopolitical confrontation, the predominance of the approach to solving conflicts and tense situations by force, the use of force , including the increased probability of using weapons of mass destruction, militarization, increased international terrorism and extremism, and intensification of mutual struggle in the information space and cyberspace.

We all understand well that the comprehensive strengthening of our country's defense capabilities and the potential of our Armed Forces is the most important condition and guarantee for the inviolability of our territories, the security and stability of our society, and the peaceful and peaceful life of our people.

These issues are of decisive importance in today's conditions, where a complex situation is emerging in the Central Asian region and the whole world, where the danger of terrorism, extremism and radicalism is increasing.

Taking this into account, we set peace and security as one of the priority areas of our activity at the very beginning of the establishment of New Uzbekistan. According to the action strategy, one of the tasks included in the set of tasks in this regard is to ensure information security and improve the information protection system, to organize timely and proportionate actions against threats in the information field.

We will bring our activities to a qualitatively new level in terms of the development of the Armed Forces and the further strengthening of the country's defense capabilities, as well as the wide

implementation of modern information and communication technologies and advanced innovations in this regard.

In particular, improving the activities of command and control bodies at all levels, increasing their level of operational and combat training in cooperation through the introduction of automated control tools and complexes, ensuring information security and cyber security will be urgent tasks in the future.

Various personal mobile devices have firmly entered the life of modern people and society. It is difficult to imagine the image of a modern person without his smartphone, tablet, laptop, smart watch, fitness bracelet and similar devices (hereafter - SHMQ). All spheres of human activity are already inextricably linked with them, including the sphere of education. At the same time, experts in the field of information security: "with the ease of use and mobility of employees, many problems and risks of information security appear."

The armed conflicts in Ukraine and Syria, especially the methods used by the online publication Bellingcat, have forced many, but primarily law enforcement agencies, to prohibit not only the use, but also the presence of SMC on the territory of special facilities, including in higher military educational institutions.

At the same time, ensuring the continuous monitoring of the implementation of such decisions is a very time-consuming process, which does not have high efficiency.

On the other hand, if a certain model of construction and management of the information security system of a special object is created, it is possible to effectively use the capabilities of the SCM, which served as a necessary condition for the emergence of prohibitions on their use, to ensure a number of problems, including information security.

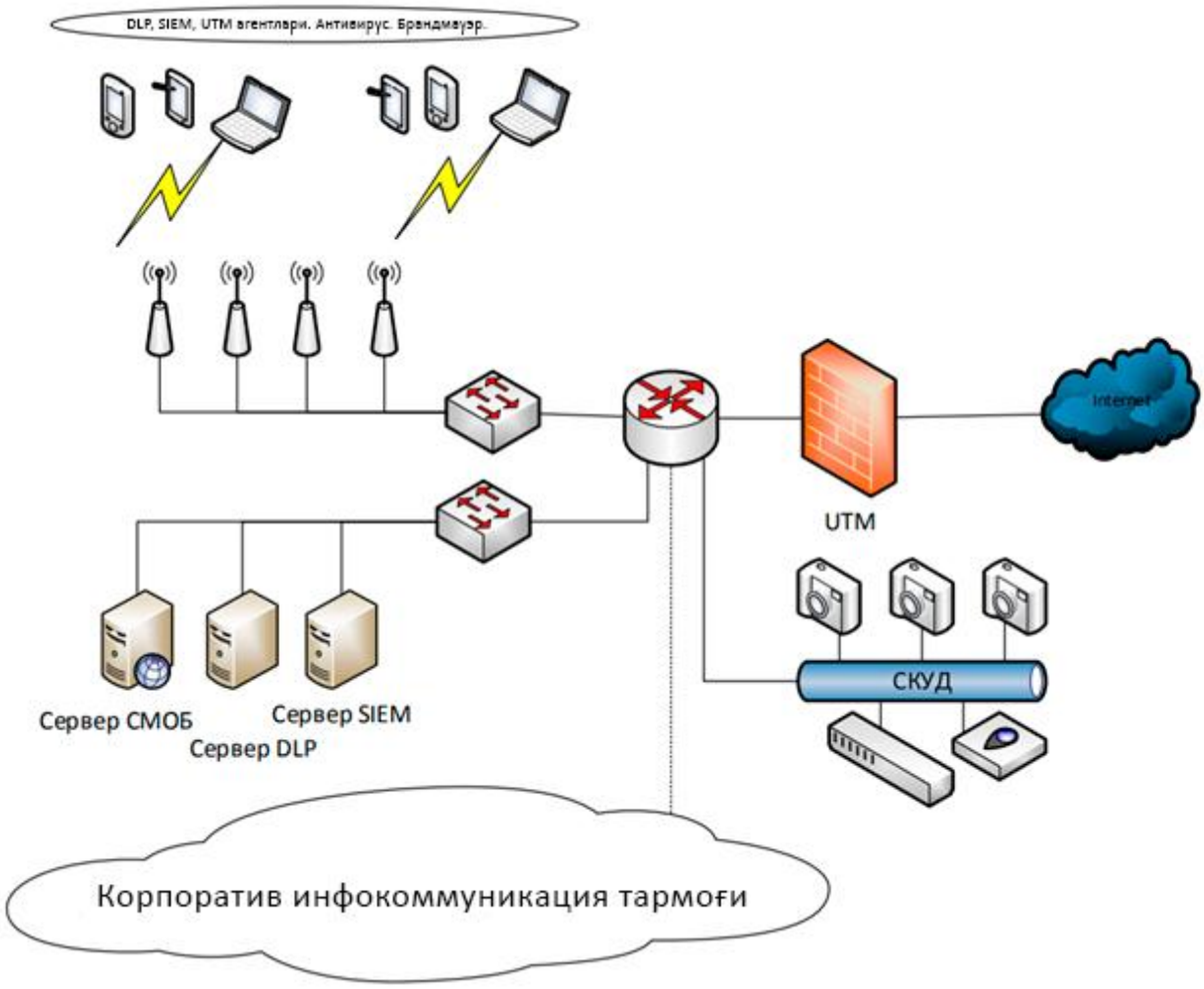
For example:

1) Monitoring the location of employees in real time (geolocation, triangulation, according to WiFi data or via cellular networks). Thus, the tragedy that happened to Aleksandar Kordzic could have been avoided as a result of using this function.
2) To take into account those who are located in the territory of ShMQ, to indicate their affiliation, location, operations carried out with its help.
3) Issuing a warning about the use of IEDs in protected areas (areas).
4) Management (management) of the used functions. For example, deleting or destroying geo-location information, banning the use of a camera, voice recorder, registering prohibited actions with issuing warnings, etc.
5) To protect the personal information of employees by monitoring and managing ShMQ's anti-virus protection, intrusion detection tools and similar programs.
6) Control of data used and processed.
7) Increase the coverage of employees by the information communication network for the purpose of management and communication.

One of the options for implementing this approach can be presented as follows (Figure 1).

This model means deploying a WiFi wireless network with an unlimited Internet connection. At the same time, a mandatory condition for user authorization is the presence of agents of security systems and specialized software used in the SMC. The network is equipped with a UTM (Unified Threat Management Unified Threat Control) system, which includes a firewall, IDS/IPS, antivirus, proxy server, content filter and anti-spam filter. DLP and SIEM systems are deployed and configured as security systems. In addition, a public safety monitoring system is being implemented based on the access control and management system operating in the facility and wireless network. Mobile DLP Server L. with server Internet UTM Server SMOB Server DLP Server SIEM, UTM agents.

Antivirus. Brandmauer. Corporate information communication network Figure 1 - model of creating an information security system.



In conclusion, it can be said that the correct configuration of these systems and their use for the benefit of the above-mentioned problems will allow to gain effective and permanent control over the channels of information flow from the SSC in higher education institutions, to reduce or eliminate the threats associated with their use.

References

1. Янги Ўзбекистон стратегияси [Матн] / Ш.М. Мирзиёев. – Тошкент: ”O'zbekiston” нашриёти, 2021. - 464 б. ISBN 978-9943-6992-3-6.
2. Ўзбекистон Республикаси Мудофаа доктринаси - Ҳарбий-сиёсий вазиятнинг ўзига хос хусусиятлари *(2018 йил 9 январь).*
3. Ўзбекистон Республикаси Мудофаа вазирининг «Ўзбекистон Республикаси Мудофаа доктринаси – мамлакатнинг ҳарбий соҳада миллий хавфсизлигини таъминлашнинг асоси» мавзусида ўтказилган илмий-амалий анжуманида “Кириш сўзи”*(2018 йил 27 январь, академия катта мажлислар зали).*
4. Печда чақирилувчи аскарнинг ўлими. (Ноябр 13, 2018). Sputnik.by дан олинган: https://sputnik.by/trend/gibelsoldata/
5. Суриядаги Россия авиабазасида унга смартфонлар михланган тахта мавжуд. (Май 23, 2018). 42.TUT.BY дан олинган: https://42.tut.by/593817 .
6. Сафонов, Л. (Б. D.). БЁД-қулайлик ва хавфсизлик. Ҳабраҳабрдан олинган: https://habr.com/company/pentestit/blog/281463.

7. Usmonov M. T. Security Models. International Journal of Academic Pedagogical Research (IJAPR) ISSN: 2643-9123 Vol. 5 Issue 1, January - 2021, Pages: 18-23.
8. Usmonov M. T. Solving Problems In Arithmetic Methods. International Journal of Academic Information Systems Research (IJAISR) ISSN: 2643-9026 Vol. 5 Issue 1, January - 2021, Pages: 58-61.
9. Usmonov M. T. Stenographic Protection of Information. International Journal of Academic and Applied Research (IJAAR) ISSN: 2643-9603 Vol. 5 Issue 1, January - 2021, Pages: 31-35.
10. Usmonov M. T. Telecommunications and Network Security. International Journal of Academic Engineering Research (IJAER) ISSN: 2643-9085 Vol. 5 Issue 1, January - 2021, Pages: 57-61.
11. Usmonov M. T. The Concept of Compatibility, Actions on Compatibility. International Journal of Academic Multidisciplinary Research (IJAMR) ISSN: 2643-9670 Vol. 5 Issue 1, January - 2021, Pages: 10-13.