The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: February 28, 2021 | **Pages:** 123-130
Doi: https://doi.org/10.37547/tajpslc/Volume03Issue02-18

IMPACT FACTOR
2021: 5. 952

Journal Website: http://usajournalshub.com/index,php/tajpslc

Training Of Personnel In The Field Of Countering Cybercrime: The Need And The Requirement Of Time

Abdulaziz Rasulev
DSc., Professor Academy Of The Ministry Of Internal Affairs Of The Republic Of Uzbekistan,

Gayrat Sadullayev
Teacher Of The Department, Prevention Of Offenses, Academy Of The Ministry Of Internal Affairs Of The Republic Of Uzbekistan

ABSTRACT

This article analyzes the issues of countering cybercrime, taking into account the dynamic development of modern information and communication and digital technologies, the impact of the Internet on the consciousness of the population, including young people, and the use of the possibilities of virtual space. The article deals with the practice of combating cybercrime and the trend of constant development of the «professionalism» of young hacker groups.

The purpose of the study is to develop proposals and recommendations, taking into account foreign experience, for further improvement of the education system, training and retraining of specialists in the field of ensuring information security of the country, countering information challenges and threats, as well as improving comprehensive measures to combat cybercrime, including in the detection, disclosure, investigation, and examination of computer crimes.

In conclusion, proposals and recommendations were developed to improve measures to counter cybercrime in universities of the Republic of Uzbekistan.

KEYWORDS

State youth policy; information and communication technologies; information security; Internet; cybercrime; youth; prevention and counteraction to computer crimes; hacker.

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: February 28, 2021 | **Pages:** 123-130
Doi: https://doi.org/10.37547/tajpslc/Volume03Issue02-18

IMPACT FACTOR
2021: 5. 952

INTRODUCTION

Today, in the international arena, the problem of combating crime in the field of information technology and security is becoming increasingly global. In particular, the UN General Assembly, the Council of Europe, the SCO, the CIS, the League of Arab States and other organizations adopted special acts related to information and communication technologies, countering and preventing the criminal use of information technologies, and preventing cybercrime in this area at the regional and international levels.

To date, the Republic of Uzbekistan has adopted 30 laws, 48 presidential acts and 84 decisions of the Government of the Republic of Uzbekistan in this area. Large-scale work is being carried out to improve the socio-political, socio-economic and judicial-legal spheres. In addition, it should be noted that efforts are being directed towards further modernizing state programs, including those aimed at countering information security and cybercrime, which include the entire range of legal, organizational, technical, and socio-political issues.

As the President of the Republic of Uzbekistan Sh.Mirziyoyev to the Oliy Majlis on December 22, 2017 «In the conditions of the current globalization, economic competition is becoming increasingly acute, information and terrorist threats are increasing. To prevent information threats and attacks through various information resources, special departments should be organized as an indispensable part of law enforcement agencies.»

First of all, I would like to draw your attention to the statistics on the development of information technologies. In the world in recent years, there has been an increase in the number of Internet users. So, in 2007, the number of Internet users in the world was 1.319 billion people, in 2015-3.263 billion people, and in 2020-4.54, and by February 1, 2021 - 4.66 billion people [4].

According to the index of development of information and communication technologies, in the world in Iceland takes the first place, the second place is occupied by Austria, third place belongs to Switzerland [12].

The number of users of social networks is growing. So, in 2010, the number of users of social networks was less than a billion people, in 2015-2.14 billion people, and in 2020 – 3.81 billion people, and by February 1, 2021 it is 4.2 billion people, which is 53.6% of the world population [9].

Statistics on the number of active actions on the Internet in one minute are of interest. So, in 2017, 3.8 million requests were made in the Google search engine, and in 2018 – 4.1, in 2019-5.2, and in 2020 - 6.3 million requests. In 2017, 3.3 million posts were posted on Facebook, and in 2018 – 3.5, in 2019 - 3.8, and in 2020 – 3.9 million posts [1].

A record growth rate in the number of Internet users in Uzbekistan was observed in 2010-2020. Their number increased from 16% to 66.7 % of the population and amounted to more than 22,102,000 people. According to statistics, 35% of Internet users use the network to use social networks, 30% of users-mail services, 25% of users-information consumption. In accordance with the data on the distribution of resources, 16% are related to education and entertainment, 9% - e-commerce and high

technologies, etc. Socio-demographic profile of Internet users: 35,1% of users are women and 64.9% are male. When it comes to their age, 36.3% are from 18 to 24, 35.1 percent of persons belong to 25 to 34 age group, 12.7% of the face from 34 to 44 years [7].

Information and communication technologies are used at all levels-individual management, economic links, and are implemented in order to ensure the internal and external security of the state. No wonder some experts believe that « a computer bomb is more dangerous than a nuclear one.» The public danger of cybercrime is characterized by a high level of economic damage caused by these types of crimes. Statistics provide information on the number of victims from cybercrime: victims per year-559 million; victims per day-more than 1.6 million; victims per second – 19 [5].

When preventing offenses on the Internet, it is necessary to pay attention to the repeated commission of offenses. So in 2020, there were 980 million offenses committed by 58 million offenders. This is more than the combined population of Switzerland, Sweden, Belgium, and Portugal [10].

Cybercrime causes damage in completely different areas of the economy: trade, competition, innovation, and generally slows down the economic growth of countries. And the more large-scale and developed country has the greater the percentage of damage from cybercrime and the greater the amount of damage caused to GDP. According to statistics for 2020, the economic damage from cybercrime was 1.23 % compared to GDP, while in this indicator, cybercrime surpassed drug trafficking (1.03 % of GDP), forgery/piracy (0.93% of GDP), (maritime piracy – 0.03% of GDP), second only to international crime and terrorism – 1.35% of GDP. It is projected that by the end of 2021, the global damage from cybercrime will reach about 2.1 trillion US dollars [6].

Experts of one of the largest foreign media companies working on IT and IT security «HACKER» claim that most hackers are just bored children who have too much free time. Only 10% of hackers are aware of their actions. 90% of acts of vandalism on the Internet are carried out by 13-year-olds who just need to «have a good time» [3]. Determining the age characteristics of Internet users also allows you to identify potential subjects who may commit crimes in the field of information technology and security. The Security Service of Ukraine has detained a hacker known by the nickname «Sanix»in Ivano-Frankivsk. At the beginning of last year, he attracted the attention of global cybersecurity experts by posting an announcement on one of the forums about the sale of a database with 773 million email addresses and 21 million unique passwords [8]. According to some reports, in 2015 in the United States, a group of young hackers (schoolchildren), which calls itself CWA, hacked the personal email of CIA Director John Brennan and Secretary of National Security Jay Johnson [15].

It should be noted that in the world practice, there is a tendency to reduce the age of the subject of crimes in the field of information technology and security. In our opinion, two reasons contribute to this:

1) The Internet has become an important and significant resource in the life of young people, an almost irreplaceable medium of communication;

2) Recently, attacks from young hackers – schoolchildren and teenagers-have begun to spread.

Given that the majority of Internet users are young people, the Internet is a very comfortable environment for the formation of a hacker's personality. In the global network, there are a number of resources designed to teach hacking skills, in particular, sites http://dfiles.ru, https://ru.wikihow.com, https://kak-bog.ru, as well as media files in the You Tube channel. In the twenty-first century, the process of institutionalization of hackers is growing rapidly, although they still strictly observe the principle of anonymity (instead of their own name, pseudonyms like «Ludichrist»are used. «Sicko», «Racket Rat», etc.). Regularly operating hacker communities are created, they have their own websites, magazines – «Access All Areas» («All Accessibility»), «Cryrt Newsletter's Home Rada» («Popular cryptographic news»), «Old and New Hackers» («Old and New hackers»), «Chaos Comuter Club» («Club of computer chaos») [13; 29-p.].

However, it should be noted that in addition to the negative links of hackers with criminal groups, recently there has been a clear trend of interaction between the hacker movement and state and commercial structures. They are attended by representatives of state security agencies, administrators of the largest companies. Moreover, some of the well-known hackers are actively involved in state and international information security organizations. For example, Andy Mueller-Megan, president and founder of the Chaos Computer Club, is a member of the world organization «ICANN» (Internet Correlation for Assigned Names and Numbers). Hacker schools of all levels are organized for children (Civil School of Hackers), students (Foundstone-shocking school) and security personnel (Black Hat Briefings, Ethical Hacking) [14].

In our opinion, this experience would be useful for the Republic of Uzbekistan. The interaction and close cooperation of hackers with state and law enforcement agencies, organizations and institutions will not only ensure the effective disclosure and prevention of cybercrimes, but also contributes to the correction of violators, their transition from the category of «offenders» to the category of «corrected» persons. In turn, practice shows that many professional hackers are excellent specialists and masters of their craft, often commit crimes out of self-interest, rarely pursuing political or other goals, and some of them commit offenses out of a sense of fun or interest. According to the 2014-2017 cybercrime research conducted by Group IB, almost all cybercrimes are aimed at obtaining financial benefits in the simplest possible way, namely, 98% of information crimes are committed out of selfish motives (theft, blackmail, extortion, fraud), 1% each – for the purpose of obtaining information and cyberterrorism, respectively [2].

This practice will be humane and innovative in the state youth policy in the country. As noted in his speech, the President of the Republic of Uzbekistan sh.Mirziyoyev at the session of the Samarkand Regional Kengash of People's Deputies of November 10, 2017 «At the same time, all of us as parents, mentors and teachers are well aware that in the current difficult and difficult time, the issue of educating young people remains the most important and urgent task for us. Therefore, we have no right to

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: February 28, 2021 | **Pages:** 123-130
Doi: https://doi.org/10.37547/tajpslc/Volume03Issue02-18

IMPACT FACTOR
2021: 5. 952

make mistakes in ensuring the legitimate rights and interests of our young people, their education and upbringing. Mistakes in this matter mean treason to our children, to the Motherland.» Therefore, the active involvement of young hackers in the activities of state and, especially, law enforcement agencies will have a positive impact on the criminogenic state in the republic.

In these conditions, social measures are becoming important, which are aimed at forming people, in particular, young people, awareness of the danger and negative consequences of crimes in the field of information technology and security.

In our opinion, the time has come to create a patriotic «Club of initiative programmers-bloggers», which will be a gathering place for talented and creative young people with the necessary knowledge and skills in the field of information and communication technologies and cybersecurity, a discussion environment and a visual platform for recruitment. In our opinion, this club is advisable to create the Union of youth of Uzbekistan and with the support of relevant Universities, Meningocele, the Ministry of innovative development with specialists, experts and analysts. In addition, the Club can be a platform for promoting and attracting young scientists to research activities in the field of cybersecurity, to promote the development of public-private partnerships through the implementation of start-up projects for the development and production of competitive products and services in the field of information and communication technologies and the digital economy, their promotion in the domestic and foreign markets. The creation of this club can serve as a vivid example of an open dialogue with young people, a kind of preventive center for the prevention and identification of persons with a tendency to commit information offenses, as well as their education in the spirit of patriotism, respect for the law and participation in the construction of a developed state and information society [11; p.198].

The main task of the state is to prepare young personnel for the conditions of life and professional activity in the information society, to teach them to act in this environment, to use its opportunities and to protect themselves from negative influences.

An important factor in countering crimes in the field of information technology and security is the level of professional training of employees of state and law enforcement agencies, information security services of organizations and institutions.

In the Republic of Uzbekistan, basic specialists in the field of information technology and information security are trained at the Tashkent University of Information Technology named after Muhammad al Khwarizmi, Inha University, AMITI University, etc. Professionals with basic legal training are preparing the Tashkent state law University, the University of world economy and diplomacy, the Islamic University, the Academy, the Academy of GBS and several faculties of other Universities. At the same time, the current trend in the field of personnel policy requires training in an interdisciplinary direction, that is, personnel with both legal and technical skills to ensure information security. In addition, the time has come to improve the system of higher education in the field of «cybersecurity», including on the basis of PPP, the creation of a program for advanced training and retraining

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
Published: February 28, 2021 | **Pages:** 123-130
Doi: https://doi.org/10.37547/tajpslc/Volume03Issue02-18

IMPACT FACTOR
2021: 5. 952

of personnel engaged in crime prevention, operational search activities, investigation and investigation of crimes related to information security and cybercrime in general.

One of particular interests is the experience of specialized educational institutions of foreign countries in the field of training specialists in the field of counteraction. investigation and disclosure of information crimes and cybercrime. For example, a number of foreign educational institutions in the EU, USA, China, India, South Korea, Russia, Belarus, and Kazakhstan train specialists in information security, radio intelligence, detection and operational and technical support for the disclosure, investigation, and prevention of cybercrime, and computer expertise in the investigation of crimes.

One of the key issues of organizing the fight against crime in information networks is the formation and improvement of the system of law enforcement agencies that can effectively solve the tasks of this fight. Law enforcement agencies have to learn «on the go» to understand new mechanisms of crimes, to look for methods of their investigation, to apply new approaches to providing electronic evidence.

Undoubtedly, the level of professional training of law enforcement agencies requires an effective and high-quality education system. The activities of law enforcement agencies to counteract crimes in the field of information technology and cybersecurity, which have a transnational and latent nature, do not meet the ever-increasing modern requirements. This state of affairs becomes possible due to the lack of qualified personnel, modern technical equipment of law enforcement agencies and expert institutions, as well as improper interdepartmental interaction of law enforcement agencies with foreign colleagues in this area. Therefore, an important task in the field of education is to improve the information infrastructure, which provides for continuous and comprehensive analysis and optimization of educational processes through the introduction of modern information and communication technologies.

One of the main directions of improving the effectiveness of the fight against cybercrime is to improve the training of relevant specialists. The study of the experience of combating cybersecurity and the analysis of universities in foreign countries in this area can contribute to improving the system of training national specialists. To date, the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan has cooperated with 14 higher educational institutions from 10 foreign countries. Signed a Memorandum on mutual cooperation with the 8 universities, including such as: the University of public security of the PRC, the Police Academy of Turkey, Barnaul law Institute of the Ministry of internal Affairs of the Russian Federation, Krasnodar University of the Ministry of internal Affairs of the Russian Federation, Volgograd Academy of the Ministry of internal Affairs of the Russian Federation, the Academy of the Ministry of internal Affairs of the Republic of Belarus, the Almaty Academy of the Ministry of internal Affairs of the Republic of Kazakhstan.

To achieve the objectives of the Universities in the country, as well as in the Academy of the Ministry of internal Affairs of the Republic of Uzbekistan the appropriate material and technical base, actively operates specialized departments and centers of information resources that are embedded in the learning

process interactive pedagogical methods of teaching created a healthy morale, well-established international academic communication.

At the same time, it should be noted that many current problems of informatization of society are not adequately covered in the process of training and retraining of young employees, which does not fully meet modern reality and the requirements of life. This alarming fact should be the object of attention of both the teaching staff of universities, law enforcement agencies, and government officials of our country, since the quality of education is not only a humanitarian problem, but also a strategic factor in the socio-economic development of the country, ensuring its national security.

In this regard, it is proposed to open a new specialized direction on the basis of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan for the training of narrow-profile specialists in the field of detection, investigation, prevention and counteraction of computer crimes in general. This specialization will allow cadets and trainees to develop scientific and practical skills in countering crimes in the field of digital technologies, cybercrime and information security.

Taking into account the scale of the problem, the dynamic growth of cybercrime in the world, as well as the emergence of real risks and threats to the entire public, especially for young people, there is a need for a radical revision of programs and methods for training and retraining specialized personnel in this field. The moment has come when society, law enforcement agencies, and national specialized universities must consolidate and respond in a timely manner to the growth of cybercrime.

REFERENCES

1. Google подвел итоги 2020 года на основе поисковых запросов [Электронный ресурс]. https://ko.ru/news/google-podvel-itogi-goda-na-osnove-poiskovykh-zaprosov/?utm_source=yxnews&utm_medium=desktop/ – Дата доступа : 18.02.2021.
2. GroupIB [Электронный ресурс]. – Режим доступа : https://psm7.com/-security. – Дата доступа : 25.06.2020.
3. Безопасность, разработка DevOps [Электронныйресурс]. – Режим доступа : https://xakep.ru/2016/07/19/13108/. – Дата доступа : 25.06.2020.
4. Вся статистика интернета на 2020 год — цифры и тренды в мире [Электронный ресурс]. https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/– Дата доступа : 18.02.2021.
5. Вся статистика интернета на 2020 год — цифры и тренды в мире [Электронный ресурс]. https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/– Дата доступа : 18.02.2021.
6. Киберпреступники вредят на триллион [Электронный ресурс] https://www.comnews.ru/content/212181/2020-12-15/2020-w51/kiberprestupniki-vredyat-trillion – Дата доступа : 18.02.2021.

7. Количество Интернет-пользователей в Узбекистане составляет 22 миллиона человек / [Электронный ресурс]. https://www.podrobno.uz/cat/tehnp/kolichestvo-internet-polzovateley-v-uzbekistane-sostavlyaet-22-milliona-chelovek/ – Дата доступа : 18.02.2021.
8. На Украине задержали укравшего рекордный объем данных хакера [Электронный ресурс]. – Режим доступа: http://www.vestifinance.ru /articles/83789. – Дата доступа : 25.06.2020.
9. Отчет по использованию социальных сетей, интернета в целом и e-commerce на начало 2021. [Электронный ресурс]. https://cpa.rip/stati/digital-2021/– Дата доступа : 18.02.2021.
10. Очередной скачок киберпреступности в 2020 году [Электронный ресурс] https://www.securitylab.ru/blog/company/CABIS/348156.php / – Дата доступа : 18.02.2021.
11. Расулев А.К. Совершенствование уголовно-правовых и криминологических мер борьбы с преступлениями в сфере информационных технологий и безопасности: диссертация … доктора юридических наук (DSc) Т. 2018 г.
12. Рейтинг стран по уровню развития информационно-коммуникационных технологий (ИКТ) [Электронный ресурс]. https://basetop.ru/reyting-stran-po-urovnyu-informatsionnyih-tehnologiy-2/ – Дата доступа : 18.02.2021.
13. Современные молодежные субкультуры: хакеры [Электронный ресурс]. – Режим доступа : http://psyfactor.org/lib/vershinin4.htm . – Дата доступа : 25.06.2020.
14. Современные молодежные субкультуры: хакеры [Электронный ресурс]. – Режим доступа : http://psyfactor.org/lib/vershinin4.htm . Дата доступа : 25.06.2020.
15. Юные хакеры «взломали» директора ЦРУ [Электронный ресурс]. Режим доступа : https://russian.rt.com/inotv/2015-10-20/CNN-YUnie-hakeri-vzlomali-direktora. – Дата доступа : 25.06.2020.