Journal scientific and applied research, vol. 16, 2019
International Journal

Original Contribution ISSN 1314-6289

IMPLEMENTATION OF THE WEB BASED PLATFORMS FOR COLLECTING AND FOOTPRINTING IP INFORMATION OF HOSTS IN THE COMPUTER NETWORK AND SYSTEMS

Petar Kr. Boyanov

DEPARTMENT OF MANAGEMENT OF SECURITY SYSTEMS, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712,115, UNIVERSITETSKA STR,

E-mail: peshoaikido@abv.bg

ABSTRACT: *In this paper implementation of the web based platforms for collecting and footprinting IP information of hosts in the computer network and systems is conducted.*

KEY WORDS: *Computer networks, DNS, Footprinting; IPv4, IPv6, LAN, Reconnaissance, Web based platforms.*

1. Introduction

The process of actively gathering information is used by malicious perpetrators (cybercriminals) mainly against employees of the target organization. The perpetrators try to get information from employees through footprinting and reconnaissance and social engineering cyberattacks such as on-site visits, interviewing, and asking different questions.

The anonymous collection of information is a process by which the malicious users collect and receive information from various sources anonymously and discreetly. This will make the tracking operation of the anonymous person completely impossible [4], [6], [9], [11].

Pseudonymously collecting information is a process of collecting publicly shared information on the Internet that does not have a direct link, and does not relate to the name (owner) of that information [12], [13], [14], [15], [16].

Thus the web based platforms for footprinting and reconnaissance find the greatest use in finding information about a victim host. These platforms are turning and connecting to the Regional Internet Registry (RIR).

This paper is structured as follows. First, in section 2, the different web based platforms for collecting and tracking IP information is performed. The achieved results are presented in section 3. The final conclusions and recommendations in section 4 are made.

2. Experiment

The science experiment in a specialized university computer lab in the Faculty of Technical Sciences at Konstantin Preslavsky was made. All of the hosts in this lab were connected each other in Local Area Network (LAN). The investigated computer network was consisted of 2 hosts. The network ID of this LAN is 194.141.47.128/26. The research host was configured with the following public IPv4 address 194.141.47.153/26.

The most used web platforms for collecting and footprinting IP information in practice are the following:

- WhatIsMyIP;
- WhatIsMyIPAddress;
- Bg whois;
- Who.is;
- Domaintools and etc.

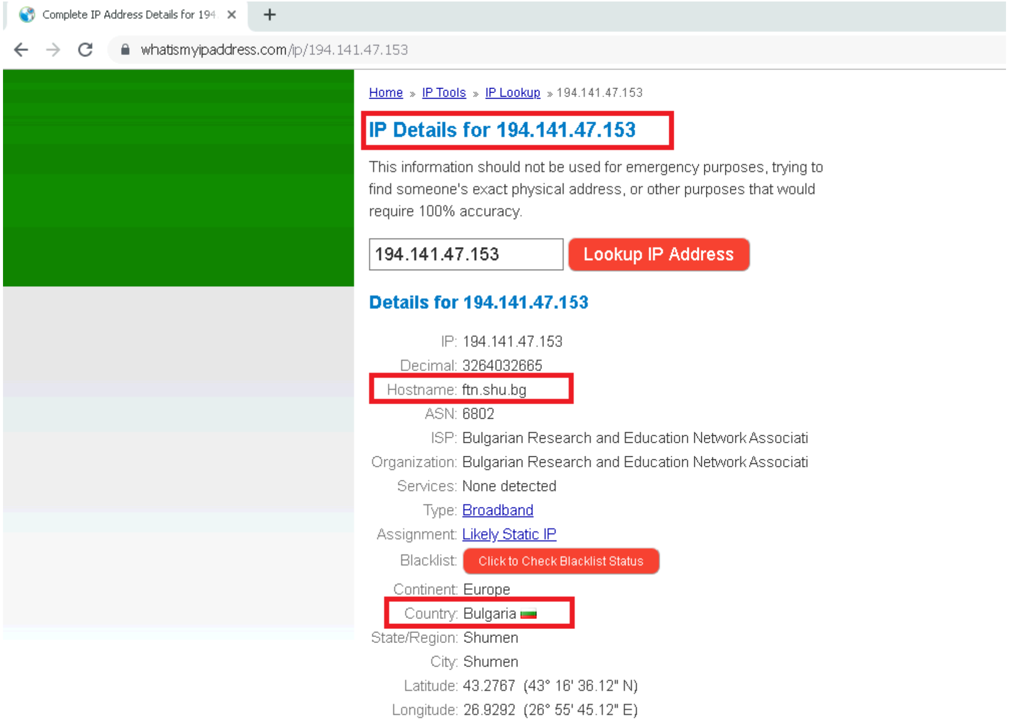
Each of the written above platform provides a large set of tools for collecting and footprinting IP address information about the target host. This set of tools includes the following services:

- IP address lookup;
- Internet speed test;
- IP Whois lookup;
- Server header check;
- Email header check;
- Domain Name System-based Blackhole List (DNSBL) or Real-time Blackhole List (RBL) check;
- Breach check;
- DNS and reverse DNS lookup;
- Proxy check;
- Port scanner;
- Hostname lookup;
- VPN leak check;
- Trace route and etc.

3. Results

Fig.1 shows the execution of the service IP lookup with the platform WhatIsMyIPAddress. It is important to note that this information should not be used for emergency purposes, trying to find someone's exact physical address, or other purposes that would require 100% accuracy.

The collected information reveals the following details as IP address (194.141.47.153), Hostname (ftn.shu.bg), Autonomous system (6802), Internet Service Provider (Bulgarian Research and Education Network Association), Organization (the same as above), Continent (Europe), Country (Bulgaria), State/Region (Shumen), City (Shumen), Latitude and Longitude coordinates, Postal code (9700). The hostname ftn.shu.bg actually is the official web site of the Faculty of Technical Sciences at Konstantin Preslavsky University of Shumen. More detailed information about the Domain Name System-based Blackhole List on fig.2 is shown. DNSBL consists of the following lists as IP nost listed (good state), IP listed (bad state), Blacklist timeout error and Blacklist offline.


Complete IP Address Details for 194
whatismyipaddress.com/ip/194.141.47.153
Home » IP Tools » IP Lookup » 194.141.47.153
Lookup IP Address
Click to Check Blacklist Status

IP Details for 194.141.47.153

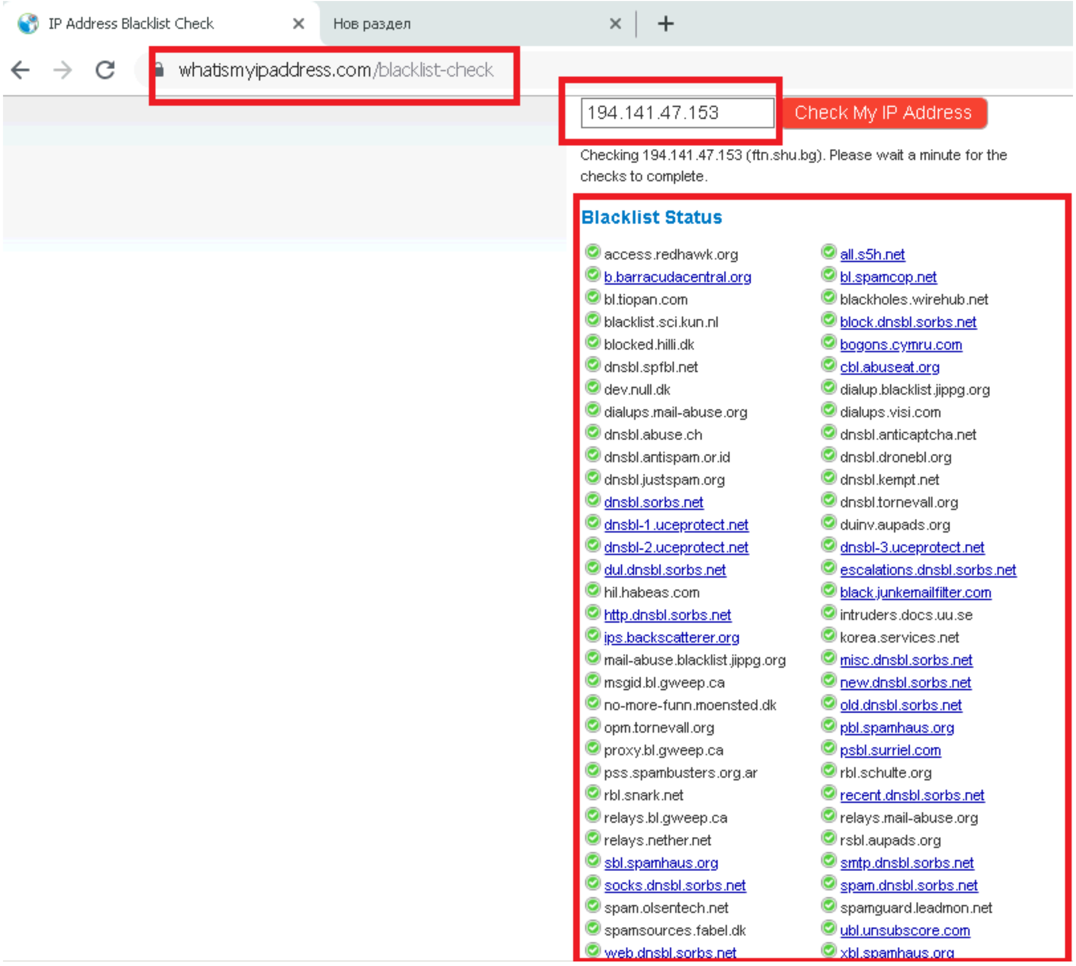
This information should not be used for emergency purposes, trying to find someone's exact physical address, or other purposes that would require 100% accuracy.

194.141.47.153

Details for 194.141.47.153

IP: 194.141.47.153
Decimal: 3264032665
Hostname: ftn.shu.bg
ASN: 6802
ISP: Bulgarian Research and Education Network Associati
Organization: Bulgarian Research and Education Network Associati
Services: None detected
Type: Broadband
Assignment: Likely Static IP
Blacklist:
Continent: Europe
Country: Bulgaria
State/Region: Shumen
City: Shumen
Latitude: 43.2767 (43° 16' 36.12" N)
Longitude: 26.9292 (26° 55' 45.12" E)

Fig. 1. The service IP lookup with the platform WhatIsMyIPAddress


IP Address Blacklist Check
Нов раздел
whatismyipaddress.com/blacklist-check
194.141.47.153
Check My IP Address

Checking 194.141.47.153 (ftn.shu.bg). Please wait a minute for the checks to complete.

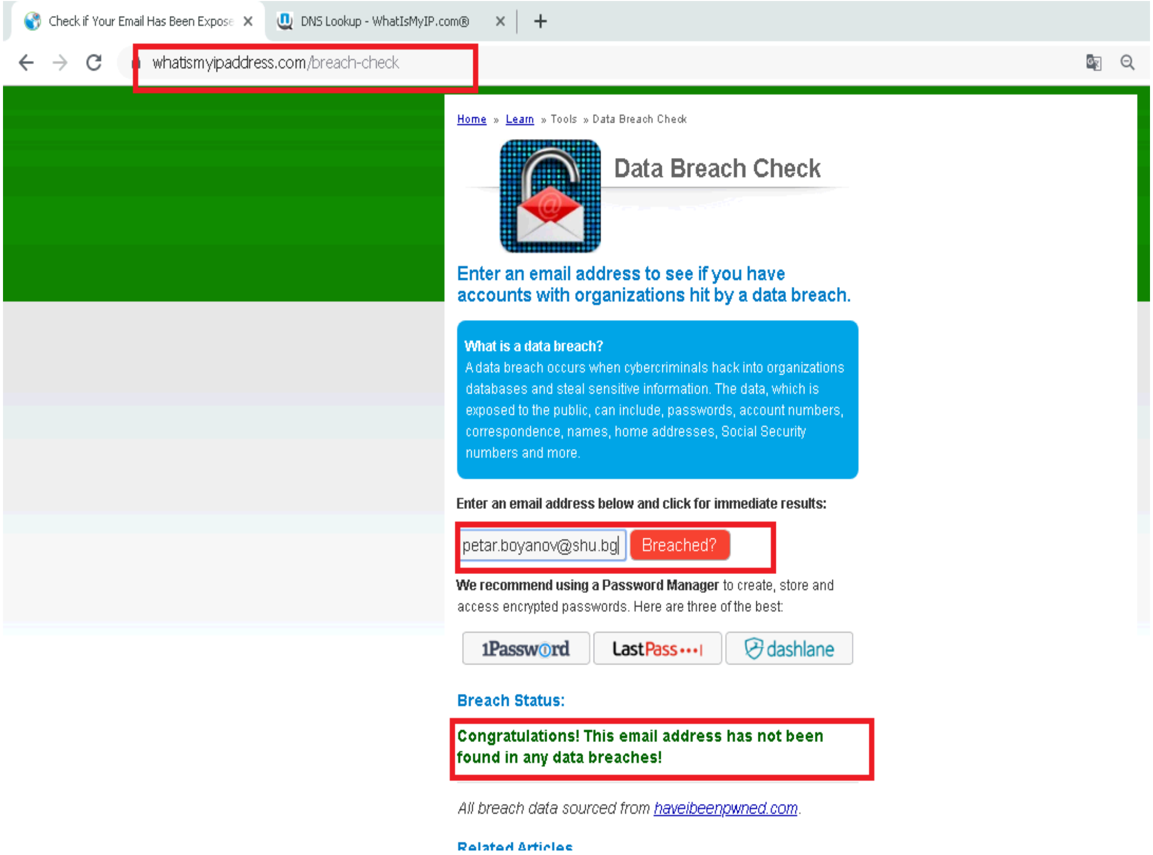
Blacklist Status

✓ access.redhawk.org
✓ b.barracudacentral.org
✓ bl.tiopan.com
✓ blacklist.sci.kun.nl
✓ blocked.hilli.dk
✓ dnsbl.spfbl.net
✓ dev.null.dk
✓ dialups.mail-abuse.org
✓ dnsbl.abuse.ch
✓ dnsbl.antispam.or.id
✓ dnsbl.justspam.org
✓ dnsbl.sorbs.net
✓ dnsbl-1.uceprotect.net
✓ dnsbl-2.uceprotect.net
✓ dul.dnsbl.sorbs.net
✓ hil.habeas.com
✓ http.dnsbl.sorbs.net
✓ ips.backscatterer.org
✓ mail-abuse.blacklist.jippg.org
✓ msgid.bl.gweep.ca
✓ no-more-funn.moensted.dk
✓ opm.tornevall.org
✓ proxy.bl.gweep.ca
✓ pss.spambusters.org.ar
✓ rbl.snark.net
✓ relays.bl.gweep.ca
✓ relays.nether.net
✓ sbl.spamhaus.org
✓ socks.dnsbl.sorbs.net
✓ spam.olsentech.net
✓ spamsources.fabel.dk
✓ web.dnsbl.sorbs.net
✓ all.s5h.net
✓ bl.spamcop.net
✓ blackholes.wirehub.net
✓ block.dnsbl.sorbs.net
✓ bogons.cymru.com
✓ cbl.abuseat.org
✓ dialup.blacklist.jippg.org
✓ dialups.visi.com
✓ dnsbl.anticaptcha.net
✓ dnsbl.dronebl.org
✓ dnsbl.kempt.net
✓ dnsbl.tornevall.org
✓ duinv.aupads.org
✓ dnsbl-3.uceprotect.net
✓ escalations.dnsbl.sorbs.net
✓ black.junkemailfilter.com
✓ intruders.docs.uu.se
✓ korea.services.net
✓ misc.dnsbl.sorbs.net
✓ new.dnsbl.sorbs.net
✓ old.dnsbl.sorbs.net
✓ pbl.spamhaus.org
✓ psbl.surriel.com
✓ rbl.schulte.org
✓ recent.dnsbl.sorbs.net
✓ relays.mail-abuse.org
✓ rsbl.aupads.org
✓ smtp.dnsbl.sorbs.net
✓ spam.dnsbl.sorbs.net
✓ spamguard.leadmon.net
✓ ubl.unsubscore.com
✓ xbl.spamhaus.org

Fig. 2. Detailed information about the Domain Name System-based Blackhole List for IP address 194.141.47.153

The Domain Name System-based Blackhole List shows that the IP address 194.141.47.153 is not listed in any blackhole list.

The service Data Breach Check provides quick results on whether an employee's email from an organization has been compromised. This may be happen when malicious users gain unauthorized access to the information resources of the organization's databases. As a result fig.3 shows that the account with email "petar.boyanov@shu.bg" has not been found in any data breaches.


Check if Your Email Has Been Expose
DNS Lookup - WhatIsMyIP.com®
whatismyipaddress.com/breach-check
Home » Learn » Tools » Data Breach Check
1Password
LastPass
dashlane
Related Articles

Data Breach Check

Enter an email address to see if you have accounts with organizations hit by a data breach.

What is a data breach?
A data breach occurs when cybercriminals hack into organizations databases and steal sensitive information. The data, which is exposed to the public, can include, passwords, account numbers, correspondence, names, home addresses, Social Security numbers and more.

Enter an email address below and click for immediate results:

petar.boyanov@shu.bg Breached?

We recommend using a Password Manager to create, store and access encrypted passwords. Here are three of the best:

Breach Status:

Congratulations! This email address has not been found in any data breaches!

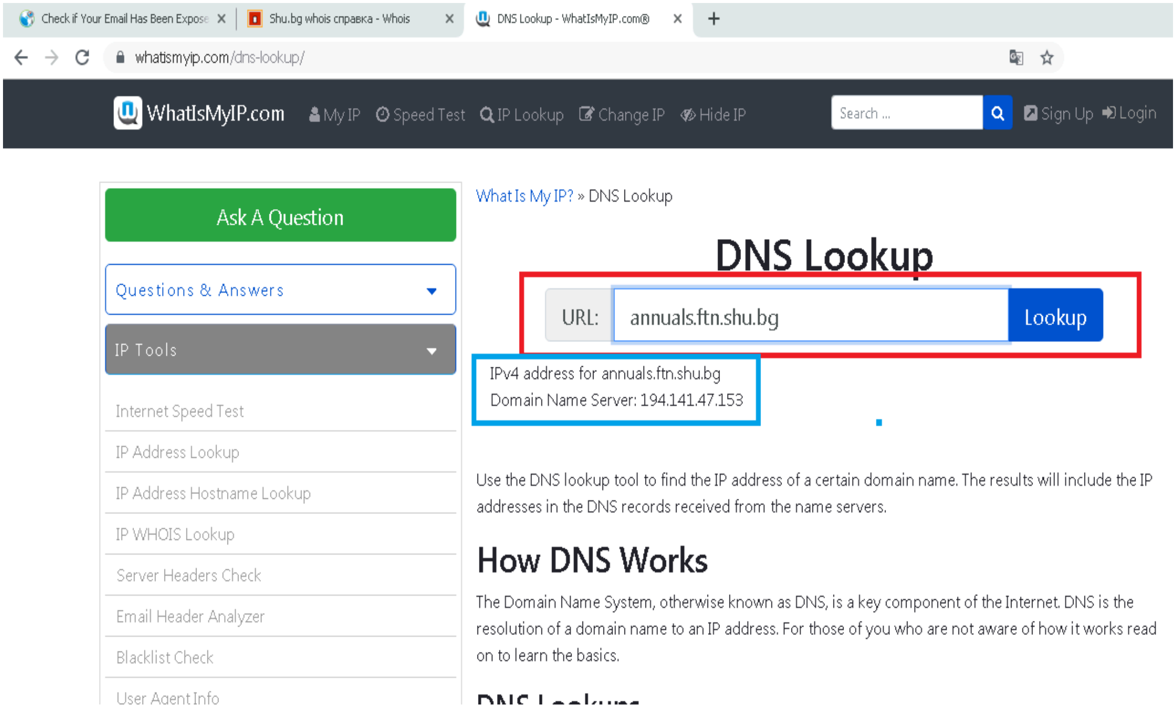
All breach data sourced from haveibeenpwned.com.

Fig. 3. Results with the service Data Breach Check

The service DNS lookup it is used to find the IP address of a certain domain name. The results will include the IP addresses in the DNS records received from the name servers. It was entered the URL of the web site - Annual of Faculty of Technical Sciences at Konstantin Preslavsky University of Shumen. As a result it was shown the Domain Name Server of this site - 194.141.47.153. This is illustrated on fig.4.

It should be noted that more than one website is hosted at this address (194.141.47.153).

The main goals of cyber-attack for obtaining information footprints and applying intelligence techniques are to collect network information, system information and information for public or private organizations [3].



DNS Lookup

URL: annuals.ftn.shu.bg

IPv4 address for annuals.ftn.shu.bg
Domain Name Server: 194.141.47.153

Use the DNS lookup tool to find the IP address of a certain domain name. The results will include the IP addresses in the DNS records received from the name servers.

How DNS Works

The Domain Name System, otherwise known as DNS, is a key component of the Internet. DNS is the resolution of a domain name to an IP address. For those of you who are not aware of how it works read on to learn the basics.

Fig. 4. Using DNS lookup for the web site annuals.ftn.shu.bg

By using web based platforms for collecting and footprinting ip information of hosts in the computer network it can be gathered sensitive information for public or private organizations as information for employees, the official or private website of the organization, organization location information, telephone numbers and addresses of employees which can be used in the Facebook app to find the employee profile and public and private IP addresses of the employees from the organization [1], [2], [5], [7], [8], [10].

NOTE: All of the scientific experiments and studies in this paper were conducted in a specialized computer lab at the Faculty of Technical Sciences at the Konstantin Preslavsky University of Shumen, consisting of several hosts. Everything illustrated and explained in this paper is for research purposes and the authors are not responsible for any misuse.

4. Conclusion

The Certified Ethical Hackers, Networks Security Officers and System Administrators have to take the following security actions and mechanisms, such as:

- Compulsory compulsion and obligation on employees not to disclose confidential information to third parties. This can be done by signing specific internal protocols to ensure that no information is disclosed to cybercriminals or competing organizations.
- Closing or blocking all unnecessary network ports in employees' computer machines through a hybrid firewall.

- Mandatory restriction or blocking of search engine access from caching on the organization or company website.
- Conducting compulsory training to improve the skills against modern types of malicious cyber-attacks.

References:

[1]. Bhattacharyya, D., Alisherov, F. Penetration testing for hire. International Journal of Advanced Science and Technology, 2009, vol. 8, pp. 1-8.

[2]. Fox, E., Bush, J., Ashley, S., Webb, I. Common Hacking Tools for Linux and Windows, 2002, CS 581 Semester Project, pp. 1-17.

[3]. Marquez, J. An Analysis of the IDS Penetration Tool: Metasploit. The InfoSec Writers Text Library, 2010, pp. 1-6.

[4]. Moore, H. D. Metasploitation. In CanSecWest Security Conference, 2006, pp. 1-28.

[5]. Shrestha, N. Security Assessment via Penetration Testing: Network and System Administrator's Approach: Security, Network and System Administrator, Penetration Testing, Master's thesis, 2012, pp. 1-98.

[6]. Hristov, H., Scanning for vulnerabilities in the security mechanisms of the hosts in the academic institutions and government agencies, Mathematical and Software Engineering, ISSN 2367-7449, Vol. 4, No. 1, 2018, pp. 1-6.

[7]. Linko Nikolov, Krasimir Slavyanov, „On the contemporary cybersecurity threats“, I st CONFSEC 2017, 11-14.12.2017, Borovets, ISSN Print: 2603-2945, ISSN Online: 2603-2953, стр. 142-144; url: http://confsec.eu/sbornik/2-2017.pdf.

[8]. Nikolov G. L., Fetfov M. O., Borisova R. A., Security concerns in javascript coding, MATTEX 2018, Volume 2, part 2, Conference proceeding, v. 2, pp. 27 – 31, Section Communication and Computer Technologies, ISSN: 1314-3921.

[9]. Nikolov G. L., Wireless network vulnerabilities estimation, International Scientific Journal “Security & Future”, Vol. 2 (2018), Issue 2, pg(s) 80-82; WEB ISSN 2535-082X; Print ISSN 2535-0668.

[10]. Nikolov, L., Slavyanov, V., Network infrastructure for cybersecurity analysis. International scientific conference 2018, “Vasil Levski” National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2018, ISSN 2367-7902.

[11]. Nikolov, L., Slavyanov, Kr., On the contemporary cybersecurity threats, Security & Future,Vol. 1 (2017), Issue 3, ISSN 2535-0668, pp.111-113.

[12]. Tsankov, Ts., Denev D. R., Use in Internet of Protocols Transport Layer Security and its now-deprecated predecessor Secure Sockets Layer. Annual of Konstantin Preslavski University of Shumen, Vol. VIII E, 2018.

[13]. Parashkevanova, G., Tsankov, Ts., Cybercrime as the main contemporary threat to large organizations, Conference proceedings Mattex 2016, ISSN 1314-3921.

[14]. Savov, I., Edin pogled varhu sashtnostta na kiberprestapleniyata, spisanie „Politika i sigurnost",VUSI, 2017, ISSN 2535-0358, s. 36-47.

[15]. Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.

[16]. Tasheva N. Zh., Bogdanov A. R., Anonymous communication system in cyberspace using tor protocol, Proceedings of Scientific Conference 2014 - Defense Technologies,Faculty of Artillery, Air Defense and Communication and Information Systems, 2014, ISBN 978-954-9681-49-9, pp. 259-265.