SECURITY PROBLEMS OF INFORMATION SOURCES STORED ON THE INTERNET

Butayeva Dilnozaxon Tulqinovna
Teacher of general secondary school No. 1, Margilan city, Fergana region
E-mail: dilnozabutaeva6@gmail.com
Jamoliddinov Raxmatilla Baxtiyor o'g'li
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
E-mail: jamoliddinovraxmatilla06@gmail.com

Annotation: *Keeping up with the burgeoning Internet of Things (IoT) requires staying up to date on the latest network attack trends in dynamic and complicated cyberspace, and take them into account while developing holistic information security (IS) approaches for the IoT. Due to multiple vulnerabilities in the IoT foundations, many targeted attacks are continuing to evolve. This survey of related work in the very specialized field of IS assurance for the IoT develops a taxonomy of typical attacks against IoT assets (with special attention to IoT device protection). Based on this taxonomy, the key directions for countering these attacks are defined. According to the modern demand for the IoT and big IS-related data processing, we propose applying the Security Intelligence approach. The results obtained, when compared with the related work and numerous analogues, are based on the following research methodology: view the IoT as a security object to be protected, leading to understanding its vulnerabilities and possible attacks against the IoT exploiting these vulnerabilities, and from there approaches to protecting the IoT. A few areas of the future research, among which the IoT operational resilience and usage of the blockchain technology seem to us the most interesting, are indicated.*

Keywords: *traffic analysis and scanning, prismdump, tcpdump, nmap, wireshark, scanrand, cain and abel, nessus, metasploit, aircrack-ng, wardriving.*

PROBLÈMES DE SÉCURITÉ DES SOURCES D'INFORMATIONS STOCKÉES SUR INTERNET

Annotation: *Pour suivre l'évolution de l'Internet des objets (IoT), il faut se tenir au courant des dernières tendances en matière d'attaques de réseau dans un cyberespace dynamique et complexe, et en tenir compte lors du développement d'approches holistiques de sécurité de l'information (SI) pour l'IoT. En raison des multiples vulnérabilités des fondations de l'IoT, de nombreuses attaques ciblées continuent d'évoluer. Cette étude des travaux connexes dans le domaine très spécialisé de l'assurance des SI pour l'IoT développe une taxonomie des attaques typiques contre les actifs IoT (avec une attention particulière à la protection des appareils IoT). Sur la base de cette taxonomie, les principales orientations pour contrer ces attaques sont définies. Conformément à la demande moderne en matière de traitement de données liées à l'IoT et au Big IS, nous proposons d'appliquer l'approche Security Intelligence. Les résultats obtenus, comparés aux travaux connexes et à de nombreux analogues, s'appuient sur la méthodologie de recherche suivante : considérer l'IoT comme un objet de sécurité à protéger, conduisant à comprendre ses vulnérabilités et les éventuelles attaques*

contre l'IoT exploitant ces vulnérabilités, et de il existe des approches pour protéger l'IoT. Quelques domaines de recherche future, parmi lesquels la résilience opérationnelle de l'IoT et l'utilisation de la technologie blockchain nous semblent les plus intéressants, sont indiqués.

Mots-Clés : *analyse et analyse du trafic, prismdump, tcpdump, nmap, wireshark, scanrand, caïn et abel, nessus, metasploit, aircrack-ng, wardriving.*

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИСТОЧНИКОВ ИНФОРМАЦИИ, ХРАНЯЩИХСЯ В ИНТЕРНЕТЕ

Абстрактный: *Чтобы идти в ногу с растущим Интернетом вещей (IoT), необходимо быть в курсе последних тенденций сетевых атак в динамичном и сложном киберпространстве и учитывать их при разработке целостных подходов к информационной безопасности (IS) для IoT. Из-за множества уязвимостей в основах Интернета вещей многие целевые атаки продолжают развиваться. В этом обзоре смежных работ в очень специализированной области обеспечения безопасности Интернета вещей представлена таксономия типичных атак на активы Интернета вещей (с особым вниманием к защите устройств Интернета вещей). На основе этой таксономии определены ключевые направления противодействия данным атакам. В соответствии с современным спросом на обработку данных, связанных с Интернетом вещей и большими информационными системами, мы предлагаем применить подход Security Intelligence. Полученные результаты по сравнению с соответствующей работой и многочисленными аналогами основаны на следующей методологии исследования: рассматривать Интернет вещей как объект безопасности, который необходимо защищать, что приводит к пониманию его уязвимостей и возможных атак на Интернет вещей, использующих эти уязвимости, и от существуют подходы к защите Интернета вещей. Обозначены несколько направлений будущих исследований, среди которых наиболее интересными нам кажутся операционная устойчивость Интернета вещей и использование технологии блокчейн.*

Ключевые слова: *анализ и сканирование трафика, prismdump, tcpdump, nmap, wireshark, scanrand, cain and abel, nessus, metasploit, aircrack-ng, wardriving.*

Unlike external reconnaissance attacks, internal reconnaissance is carried out on the spot. This means that attacks are carried out within an organization's network, systems and premises. This process is mainly assisted by software. The attacker interacts with real target systems to obtain information about their vulnerabilities. This is the main difference between the methods of internal and external intelligence

External intelligence is carried out without interaction with the system, by searching for entry points through people who work in the organization. This is why most foreign intelligence attempts involve hackers trying to contact users through social media, email

and phone calls. Insider intelligence is still a passive attack because the goal is to find information that can be used later to carry out an even more serious attack.

The main goal of internal intelligence is the internal network of the organization, where hackers will definitely find data servers and IP addresses of hosts that they can infect. It is known that data on a network can be read by any user on the same network with the right set of tools and skills. Attackers use networks to discover and analyze potential targets for future attacks. Internal intelligence is used to identify security mechanisms that prevent hacking attempts. There are many cybersecurity tools that have been created to neutralize software used to carry out intelligence attacks. However, most organizations never install enough security controls, and hackers continue to find ways to compromise those already installed. There are a number of tools that have been tested by hackers and proven proven to be effective in studying victim networks. Most of them can be classified as traffic analysis tools.

Traffic analysis and scanning

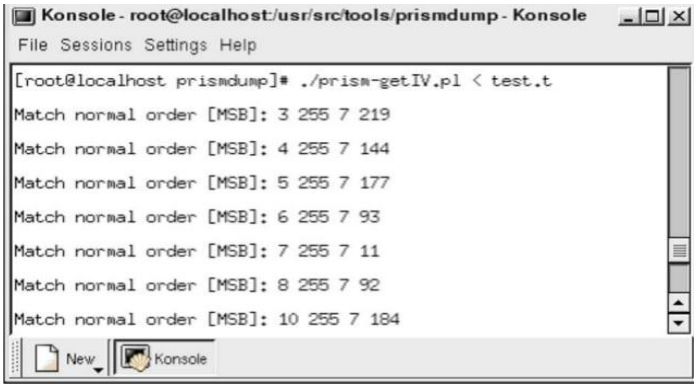
These terms, when used in a network environment, usually refer to eavesdropping on traffic on a network. They allow attackers and defenders to know exactly what is happening on the network. Traffic analysis tools are designed to capture packets transmitted over a network and analyze them, which is then provided in a human-readable format. For internal intelligence, packet analysis is more than necessary. It gives attackers a wealth of information about the network, which can be compared to reading the logical layout of the

Some sniffing tools can reveal sensitive information, such as passwords from Wi-Fi encrypted networks

WEP. Others allow hackers to intercept traffic on wired and wireless networks for long periods of time, after which they can conduct analysis at their discretion. Today, there are many tools that hackers use.

Prismdump

Designed exclusively for Linux, this tool allows hackers to analyze the traffic of cards based on Prism2 chipsets. This technology is designed to capture packets only, leaving the analysis to other tools. This is the reason why this tool saves recorded packets in pcap format, which is widely used by other traffic analysis tools. Most open source tools use pcap as a standard saved packet format. Since this utility is intended only for data collection, it is reliable and can be used for long reconnaissance missions In screenshot of prismdump.



Tcpdump

It is an open source traffic analysis tool that is used to capture and analyze packets. tcpdump uses the command line interface. It was specifically designed for packet recording because it does not have a graphical user interface to analyze and display data. This tool has one of the most powerful packet filtering capabilities and can even record packets selectively, which sets it apart from most other traffic analysis tools that do not have packet filtering capabilities during capture. Below is a screenshot of tcpdump (Figure 4.4). On it, it listens for ping commands sent to his host

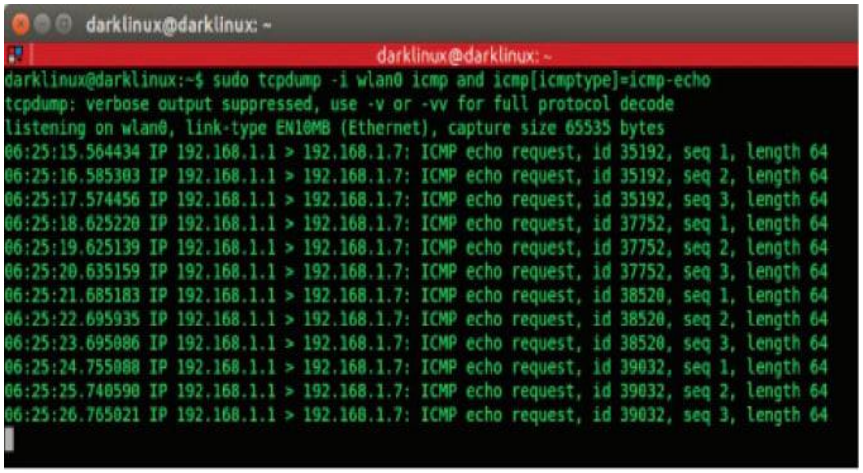


Fig. 4.4

Nmap

It is an open source network code analysis tool that is commonly used to build a network map. It records IP packets entering and leaving the network and also displays detailed information about the network, such as devices connected to it and any open and closed ports. NMap can even determine the operating systems of devices connected to the network, as well as firewall configurations. It uses a simple text interface, but there is an advanced version called Zenmap that also has a GUI. Below is a screenshot of the nmap interface. Executed command:

#nmap 192.168.12.3

This command is used to scan computer ports by IP address. resu 192.168.12.3 (Fig. 4.5).

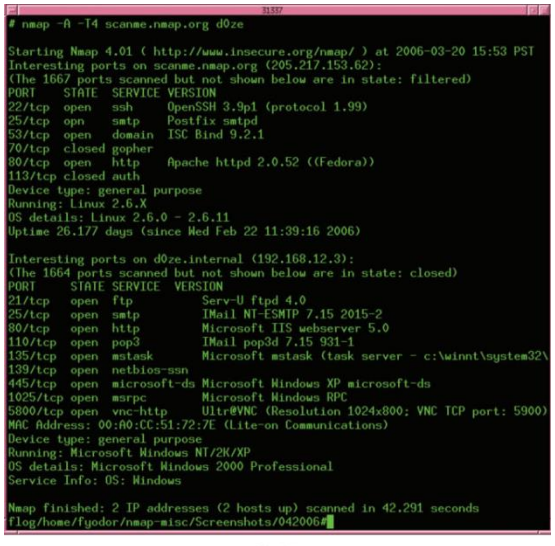


Fig. 4.5

Wireshark

It is one of the most respected utilities used for network scanning and sniffing. It is so powerful that it can steal authentication details from traffic sent from the network (1). It's surprisingly easy to do, so you can easily become a hacker by simply following a few steps. On Linux, Windows and Mac you need to make sure that the device where you installed Wireshark (preferably laptop), connected to the network. Wireshark must be running to be able to capture packets. After a specified period of time, you can stop Wireshark and begin performing analysis. To obtain passwords you need to filter collected data so that only POST request data is displayed, because most sites use POST to pass authentication information to their servers. It will list all the actions performed on the POST data. Then right click on any of them and select the option to follow the TCP stream. Wireshark will open a window with your username and password. At times, the captured password is hashed, and this often occurs on websites. You can easily compromise the hash value and recover the original password using other utilities.

Wireshark can also be used for other functions, such as recovering passwords from Wi-Fi networks. Since it is open source software, the community is constantly updating its capabilities and will therefore continue to add new features. Its current main features include capturing packets, importing pcap files, displaying protocol information about packets, exporting captured packets in several formats, filter-based packet coloring, providing network statistics, and the ability to search through captured packets. The file has advanced capabilities, which makes it ideal for hacking. The open source community, however, uses it for "white hat" hacking, which discovers vulnerabilities in networks before black hat hackers do.

In Fig. 4.6 shows a screenshot of Wireshark, which captures network pas

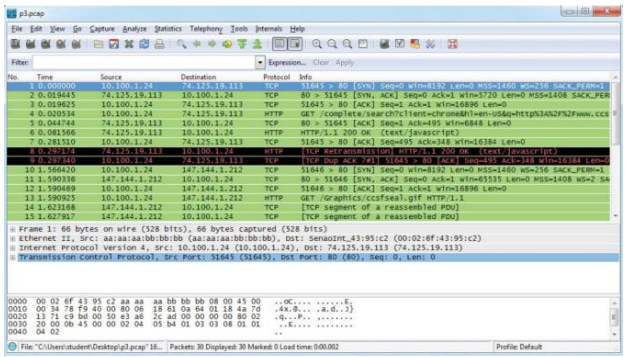


Fig. 4.6

Scanrand

This is a purpose-built scanning tool that is extremely fast yet effective. It is superior to most other scanning tools due to its high speed, which is achieved in two ways. This utility runs a process that sends multiple requests simultaneously and a process that receives responses and integrates them. The two processes do not coordinate their actions, and therefore one can never know exactly what to expect, except that there will be response packets

However, there is a clever method based on message hashing, which is integrated into Scanrand. It allows you to view the actual scan responses. Scanrand is completely different

from older scanning tools such as NMap. Its enhancement allows it to capture packets faster and more efficiently.

Cain and Abel

This is one of the most effective password cracking tools designed specifically for the Windows platform. It recovers passwords by cracking them using dictionary attacks, bruteforce attacks, and cryptanalysis. It also analyzes network traffic, listening to conversations in VoIP applications and detecting cached passwords. Cain and Abel has been optimized to work only with Microsoft operating systems. In Fig. 4.7 shows a screenshot.

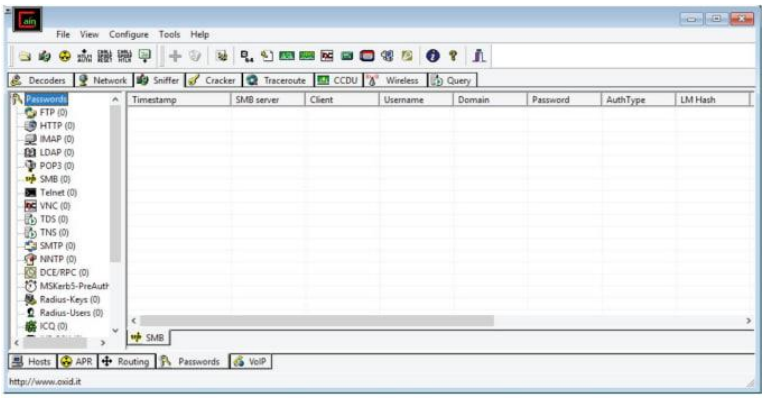


Fig. 4.7

Nessus

This is a free scanning tool created and distributed by Tenable Network Security. It has been ranked among the best network scanners and has received several awards as the best vulnerability scanner for white hat hackers. Nessus has a number of functions that can be useful to an attacker engaged in internal intelligence. The tool can scan the network and show connected devices that have incorrect configurations and missing patches. Nessus also shows devices that use default passwords, weak passwords, or no passwords at all.

It can recover passwords from some devices by running an external tool to help it with dictionary attacks on targets on the network. Finally, this tool is capable of displaying anomalous traffic on the network, which can be used to monitor DDoS attacks. Nes-sus has the ability to call external tools to achieve additional functionality. When it begins scanning the network, it can turn to NMap to scan for open ports, and will automatically aggregate the data that NMap collects. Nessus can then use this type of data to continue scanning and finding additional information about the network using commands written in its language. In Fig. Figure 4.8 shows a screenshot of Nessus with a scan report.

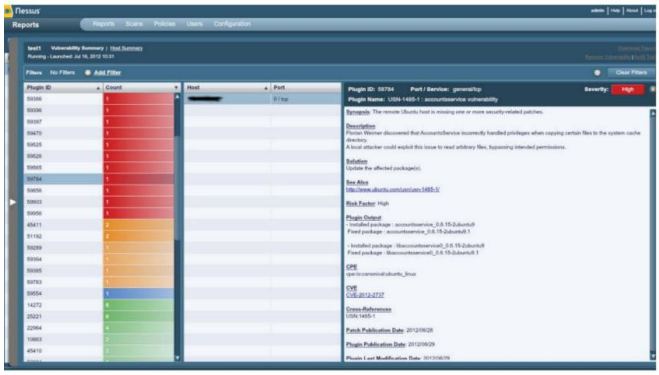


Fig. 4.8

Metasploit

This is a legendary framework consisting of a number of tools that are used to scan and exploit networks. Due to the wide capabilities of this tool, most instructors, “white hackers”, use it to transfer knowledge to their students. It is also used for penetration testing and is the software of choice in a number of organizations. At the moment, this framework has over 1500 exploits that can be used for browsers, Android, Microsoft, Linux and Solaris operating systems, and there are also some other exploits applicable to any platform.

Metasploit deploys its payloads using a shell, meterpreter, or dynamic payloads.

The advantage of Metasploit is that it has mechanisms that detect and evade security programs present on the network. The framework has several commands that can be used to analyze information from networks, as well as additional tools that can be used for exploitation after collecting information about the vulnerability.

In Fig. 4.9 shows screenshots of Metasploit.

Aircrack-ng

Another tool for scanning wireless networks is Aircrack-ng. It is specifically used to hack secure wireless networks. This is an advanced tool. It has algorithms that can break into secure wireless networks with WEP, WPA and WPA2 encryption (1). It has simple commands, and even a novice can easily compromise a secure network with WEP encryption. Aircrack-ng's potential comes from its combination of FMS, Korek and PTW attacks. They are very successful in the algorithms used to encrypt passwords.

FMS is typically used against RC4 encrypted passwords. WEP is attacked using Korek. WPA, WPA2 and WEP are subject to PTW attacks. Aircrack-ng works thoroughly and almost always guarantees login to networks that use weak passwords.

In Fig. 4.10 shows a screenshot of it.

Wardriving

This is an indoor intelligence technique used specifically for surveying wireless networks. It is usually carried out from a car and is aimed mainly at unprotected networks. There are several tools that have been created for wardriving. The most common are network stamblers and mini-stamblers. The network installer is based on Windows. It records the SSIDs of unsecured wireless networks before using GPS satellites to record the exact location of the wireless network water network. The data is used to create a map that other wardrivers use to find unsecured or insufficiently secure wireless networks. They can then exploit the network and its devices, since entry is free.

Mini Stacker is a similar tool, but it is designed to work on tablets and smartphones. This makes wardrivers appear less suspicious when identifying or exploiting a network. The utility will simply find an unprotected network and record it in the online database. Later, wardrivers will be able to exploit the network using a simplified map of all identified networks. In the case of Linux, you can use Kismet.

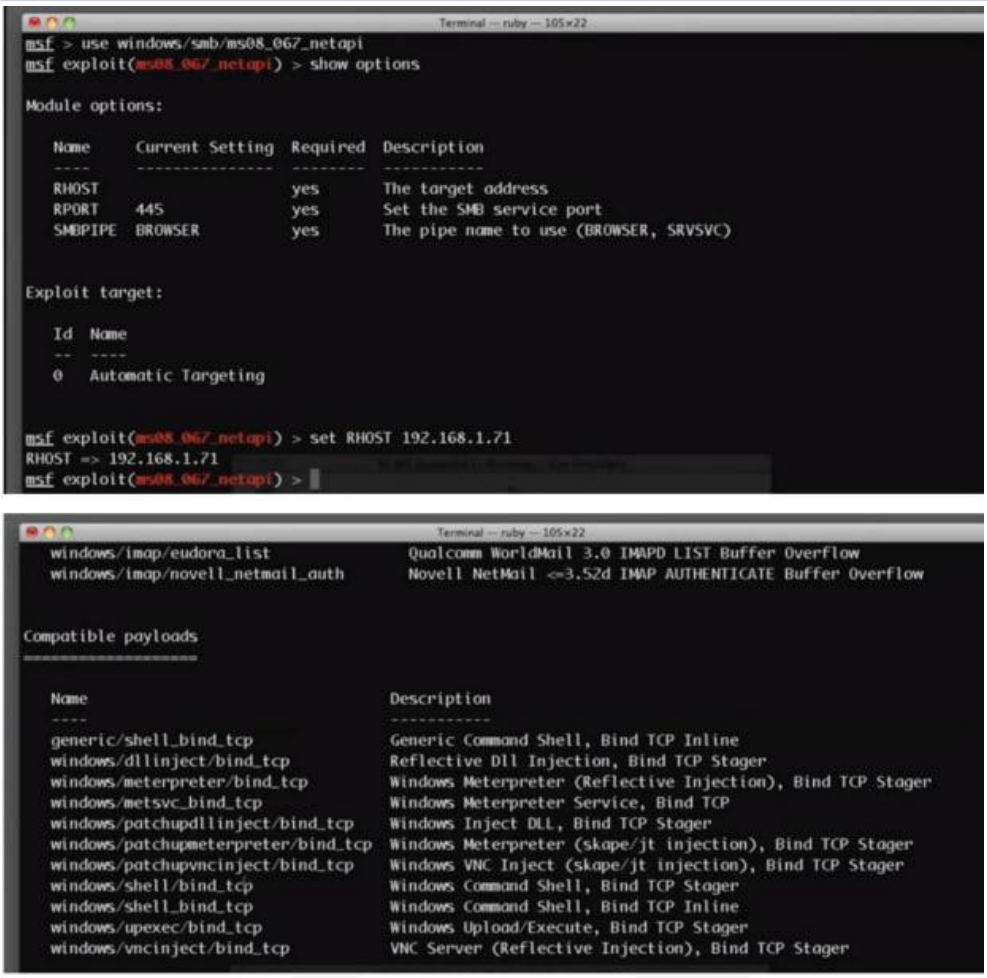


Fig. 4.9

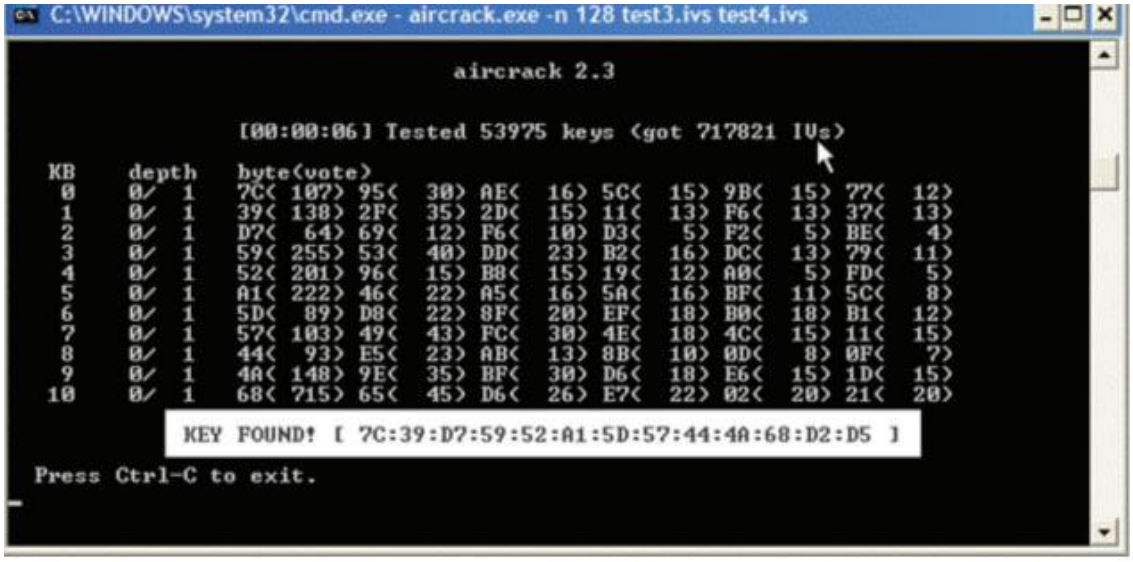


Fig. 4.10

This tool is considered very powerful as it lists unsecured networks and details of clients on networks such as BSSID, signal levels, and IP addresses. It can also list identified networks on maps, allowing attackers to come back and attack the network using known information. First of all, it monitors traffic via 802 11- channel protocols on a Wi-Fi network and uses any Wi-Fi adapter on the computer on which it was installed

ФОЙДАЛАНГАН АДАБИЁТЛАР:

1. Jamoliddinov, Raxmatilla, and Maftuna Sultonova. "ПОТЕНЦИАЛ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ И УМЕНЬШЕНИЯ ПРЕСТУПНОСТИ." Наука и технология в современном мире 2.18 (2023): 4-11.

2. Paula de M. One Man's Trash Is... Dumpster-diving for disk drives raises eyebrows // U.S. Banker. 2004. № 114 (6). C. 12. https://search.proquest.com/docview/ 200721625.

3. J. Brodkin. Google crushes, shreds old hard drives to prevent data leakage // Network World. 2017. http://www.networkworld.com/article/2202487/data-center/google-crushes-shreds-old-hard-drives-to-preventdata-leakage.html.

4. Brandom. Russian hackers targeted Pentagon workers with malware-laced Twitter messages // The Verge. 2017. https://www.theverge.com/2017/5/18/15658300/ russia hacking-twitter-bots-pentagon-putin-election

5. Swanson A. Identity Theft, Line One // Collector. 2008. № 73 (12). C. 18–22, 24–26. https://search.proquest.com/docview/223219430.

6. Gupta P., and Mata-Toledo R. Cybercrime: in disguise crimes // Journal of Information Systems & Operations Management. 2016. C. 1–10. https://search.

a. proquest.com/docview/1800153259.

b. Gold S. Social engineering today: psychology, strategies and tricks // Network

c. Security. 2010. № 2010 (11). C. 11–14. https://search.proquest.com/docview/

7. 787399306?accountid=45049. DOI: http://dx.doi.org/10.1016/S1353-4858(10) 70135-5.

8. Anderson T. Pretexting: What You Need to Know // Secur. Manage. 2010. № 54 (6). C

9. https://search.proquest.com/docview/504743883.

10. Harrison B., Svetieva E., and Vishwanath A. Individual processing of phishing emails // Online Information Review. 2016. № 40 (2). C. 265–281. https://search. proquest.com/docview/1776786039.

11. Каршиев У. Х. и др. ZAMONAVIY ICHKI ISHLAR ORGANI HODIMLARIDA CHET TILLARINI O'RNI VA AHAMIYATI! //INNOVATION IN THE MODERN EDUCATION SYSTEM. – 2023. – Т. 3. – №. 29. – С. 493-500.

12. Top 10 Phishing Attacks of 2014 – PhishMe // PhishMe. 2017. https://phishme.com/top-10-phishing-attacks-2014/. Amir W. Hackers Target Users with 'Yahoo Account Confirmation' Phishing

13. Email // HackRead. 2016. https://www.hackread.com/hackerstarget-users-withyahoo-account-confirmation-phishing-email/.

14. Dooley E. C. Calling scam hits locally: Known as vishing, scheme tricks people into giving personal data over phone // McClatchy – Tribune Business News. 2008. https://search.proquest.com/docview/464531113. Hamizi M. Social engineering and insider threats // Slideshare.net. 2017. https:// www.slideshare.net/pdawackomct/7-social-engineeringand-insider-threats. Hypponen M. Enlisting for the war on Internet fraud //

CIO Canada. 2006. № 14 (10). C. 1. Available: https://search.proquest.com/docview/217426610.

15.Baxtiyor o'g'li, Jamoliddinov Raxmatilla. "O 'ZBEKISTONDA REFERENDUM O 'TKAZISHINING AKTUALLIGI." Journal of Universal Science Research 1.4 (2023): 564-567.

16.Duey R. Energy Industry a Prime Target for Cyber Evildoers // Refinery Tracker. 2014. № 6 (4). C. 1–2. https://search.proquest.com/docview/1530210690.

17.Chang J. J. S. An analysis of advance fee fraud on the internet // Journal of Financial Crime. 2008. № 15 (1). C. 71–81. https://search.proquest.com/docview/235986237?accountid=45049. DOI: http://dx.doi.org/10.1108/13590790810841716.

18.Packet sniffers – SecTools Top Network Security Tools // Sectools.org. 2017. http://sectools.org/tag/sniffers/