



Assessment Of Students Cybersecurity Awareness And Strategies To Safeguard Against Cyber Threats

Vishal Verma^{1*}, Janardan Pawar²

^{1,2} Indira College of Commerce and Science, Pune.
Email: mca.vishalverma@gmail.com¹, janardanp@iccs.ac.in²

***Corresponding Author:** Vishal Verma
Email: mca.vishalverma@gmail.com

Abstract

This paper attempts to examine the extent of cybersecurity awareness among college students and propose some effective measures to prevent them from cyber-attacks. In light of the pervasive integration of cutting-edge technologies in education and our daily life, College students faces various on-line threats. Given their active internet usage, college students are particularly susceptible to cyber-attacks through activities such as exploring e-content, engaging in social media platform, participating in online learning platforms, digital polls, quizzes, Kahoot, online debates and research work. This study holds significance for college students, who are particularly vulnerable. To protect them from cyber threats, understanding their level of cybersecurity consciousness regarding phishing scams, malware, ransomware, and other computer threats, as well as their knowledge of preventive measures, is extremely crucial. The escalating number of hackers and organized cybercriminals underscores the need for heightened cybersecurity awareness. These cybercriminals continually seek innovative techniques for cyber theft, including obtaining sensitive and confidential information from college students for potential blackmail or selling to others. This study involves an efficient online survey conducted among college students to gauge their cybersecurity awareness and preventive measures knowledge. Based on the survey findings, recommendations are provided to strengthen cybersecurity and encourage safer online practices among college students.

CC License
CC-BY-NC-SA 4.0

Keywords: *Cybersecurity, Cyber-Attacks, Malware, Ransomware, Phishing.*

1. Introduction

The surge in technological expertise has brought numerous benefits, yet concurrently exposed internet users to diverse various cyber threats. In the contemporary landscape, imagining any task without digital devices is difficult, as these devices have replaced traditional working systems across various sectors such as education, offices, and retail spaces. The ubiquity of digital devices in all facets of the economy is undeniable. While

this remarkable invention has become an integral part of our day to day lives, individuals accessing information through these devices often overlook essential security measures during online activities, thereby neglecting the associated upcoming cyber threats. The continuous integration of new technologies and networking devices has led to an annual increase in cyberattacks. Cybercriminals are relentless in developing sophisticated tactics to breach security and access private, sensitive information with the intent to cause harm. This study aims to evaluate the level of cybersecurity awareness among college students and proposes effective measures to mitigate cyber risks, addressing the wide array of sectors that students often overlook in their day-to-day activities. The recommendations presented in this research paper aim to provide individuals with the knowledge to operate digital devices cautiously, offering guidance on securing them through specified steps outlined in the research.

2. Objectives

This paper proposes various recommendations to safeguard against cyber-theft and serving as a helpful resource for internet users, particularly college students. The recommended security measures are not only cost-effective but also ensure the protection of sensitive and confidential data. The proposed system enhances student awareness through the implementation of various techniques presented as recommendations.

The primary objectives are:

- To identify the cyber security awareness among students through survey.
- To analyze the gathered data to find out the awareness ratio among students.
- To make students understand to promote security.
- To provide some strategies to safeguard against cyber threats.

3. Literature Review

While concluding the study literature review has been taken as follows:

Abomhara, M., & Kjøien, G. M. (2015) The rapid growth of Internet of Things (IoT) devices and services is accompanied by a growing number of threats and attacks directed at these IoT systems. Although instances of cyber-attacks on IoT have been noted previously, the widespread integration of IoT into various aspects of our lives underscores the need to prioritize cybersecurity measures. Consequently, there is a vital need to strengthen the security of IoT and gain a comprehensive understanding of the threats and attacks directed at IoT infrastructure. This paper seeks to categorize various types of threats, as well as analyze and characterize intruders and attacks faced by IoT devices and services. [1]

Alexei, L. A. and Alexei, A. (2021) A detailed investigation was conducted to create an effective mapping study that explores prevalent cybersecurity vulnerabilities. Through an in-depth analysis of numerous primary studies, valuable insights were gained into the frequency of these vulnerabilities. The research underscores the constraints of current security approaches and their real-world applications. Additionally, it emphasizes the imperative for future research to identify and tackle other noteworthy cybersecurity vulnerabilities pertaining to specific applications, mitigation strategies, and infrastructures. [2].

Alshayeb, M. et.al. (2020) The field of cybersecurity has experienced a notable increase in research efforts dedicated to bolstering cyber applications and addressing major security challenges they encounter. This study aims to systematically trace and assess the prevalent vulnerabilities in cybersecurity. To fulfill this goal, a systematic mapping study was executed, involving the identification and analysis of 78 primary studies. Furthermore, the analysis indicates that a significant portion of the studies chosen for this review concentrates on a restricted range of commonly encountered security vulnerabilities, including phishing attacks, malware, ransomware, and denial-of-service incidents. [3].

Nikhita Reddy Gade and Ugander G J Reddy (2014) In the field of information technology, the significance of Cyber Security is crucial for protecting data, posing a considerable challenge in the contemporary world. Governments and organizations globally are adopting numerous strategies to counter the escalating cyber threats. Despite these endeavors, Cyber Security remains a substantial worry. This paper primarily addresses the obstacles faced by Cyber Security in light of the latest technologies. It also delves into recent advancements in Cyber Security methodologies, ethical considerations, and emerging trends that shape the landscape of security in the cyber domain. [4].

Eric C. K. Cheng and Tianchong Wang (2022) The pressure of cybersecurity threats has imposed a substantial burden on organizations, and Higher Education Institutions (HEIs) are especially susceptible.

Nevertheless, current cybersecurity research often lacks practical relevance for leaders and policy-makers in HEIs, often focusing narrowly on technology. Best practice publications often fall short in offering a comprehensive, system-wide outlook on cybersecurity within HEIs. This paper seeks to address this literature gap by developing institutional cybersecurity strategies from a holistic standpoint. [5].

Thakur, K., Qiu, M. K. et.al. (2015). The research paper concentrates on cybersecurity threats and security models, investigating the challenges and potential solutions in this domain. Its aim is to offer a thorough comprehension of diverse cyber threats and the security models available for addressing them. The author outlines existing security paradigms and endeavors, providing a summary of the issues related to cybersecurity threats. [6]

4. Research Methodology

A comprehensive survey was developed and distributed to students across various colleges and disciplines in the Pune region. The survey covered topics such as digital device usage, cybersecurity awareness, online behaviors, experiences with cyber threats, awareness of preventive measures, and the implementation of security measures. The collected data underwent analysis to discern trends and gaps in cybersecurity. The analytical survey, conducted in multiple educational institutions in Pune, provided insights into the awareness levels regarding security measures during online activities. The online survey was conducted ethically, ensuring a well-organized approach and a large, diverse sample of male and female college students. Findings indicated varying levels of cybersecurity awareness among the participants. While the majority displayed basic knowledge, such as understanding passwords, there was a lack of comprehension regarding more intricate threats. Students exhibited uncertainty about concepts like malware, ransomware, identifying phishing attempts, and the importance of firewalls and antivirus software. Furthermore, a significant portion of the respondents was unaware of the risks associated with using public Wi-Fi networks, and many shared personal information without considering potential consequences.

As per to Figure (a), the survey conducted via a poll indicates a notably low level of security awareness. The results reveal that 47 percent of students are cognizant of proper security measures but fail to implement them, thereby exposing themselves to risks. Additionally, 31 percent of students are both cognizant and have implemented security measures to some extent. However, 22 percent of students lacking awareness of necessary security measures, placing them at a high risk of potential threats.

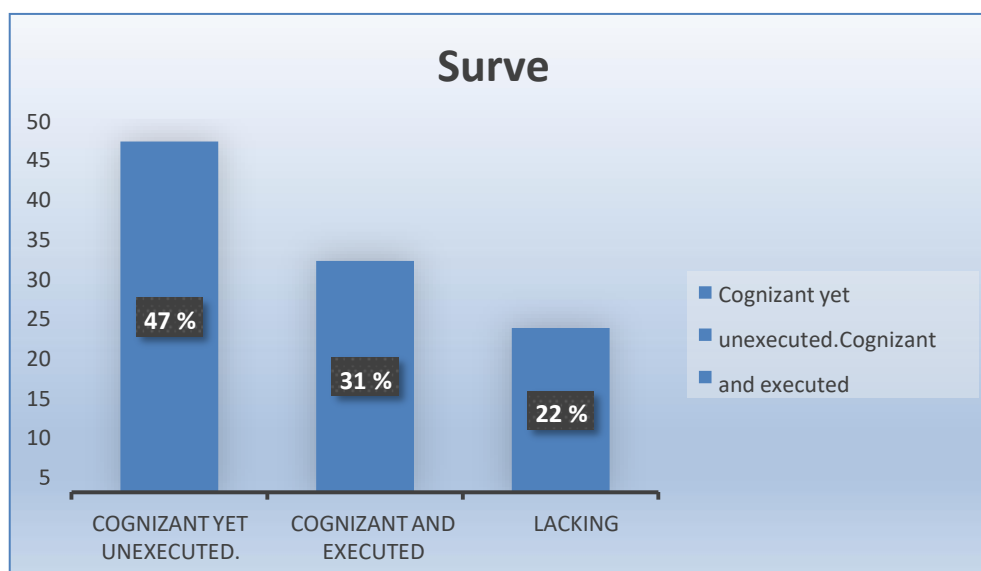
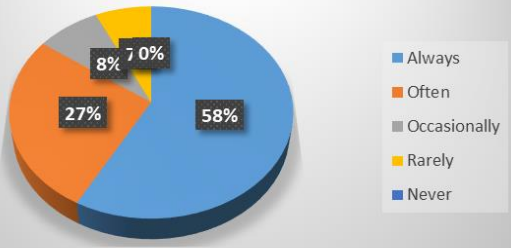
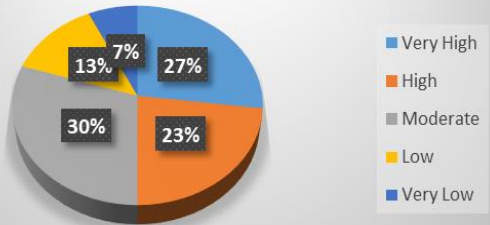
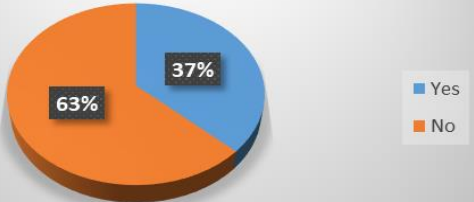
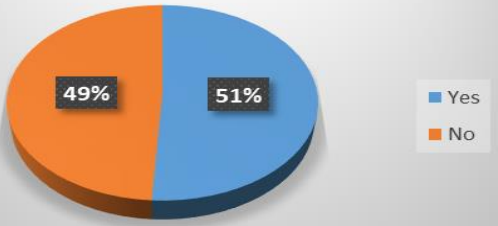
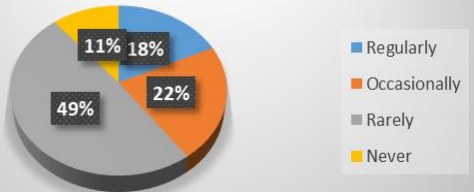
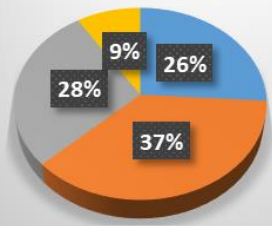
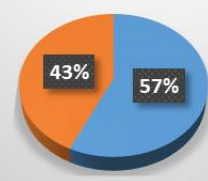
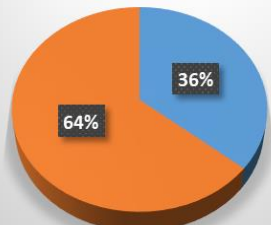
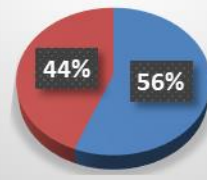
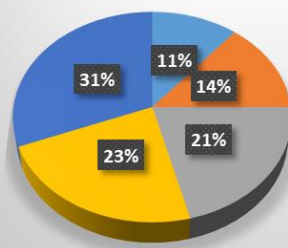


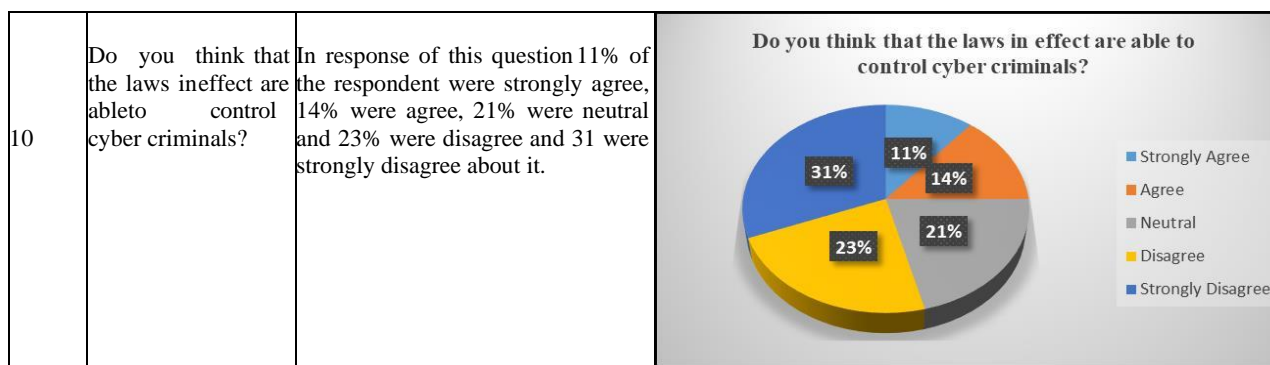
Figure (a)

To find the relevant statistics and analysis the Questionnaire prepared which consists of the questions illustrating the rise in cyber threats targeting Sample Size taken for the analysis is approximate 112 students who are also internet users on the awareness of cybercrimes in the "Pune", region The age of the respondents falls between 18 to 30 years and where 62 boys and 49 girls. Convenience sampling method was adopted to select the respondents for the survey In this research, attempt to concentrate on the significance of measuring the cyber security awareness of students by answering the following questions:

Detailed Analysis of Survey

Sr. No.	Question	Analysis	Graphical Result												
1	How frequently do you use the internet?	In response of this question 58% of the respondent were always use, 27% were often use, 8% were Occasionally and 7% were rarely use the Internet.	<p>How frequently do you use the internet?</p>  <table border="1"> <tr><th>Frequency</th><th>Percentage</th></tr> <tr><td>Always</td><td>58%</td></tr> <tr><td>Often</td><td>27%</td></tr> <tr><td>Occasionally</td><td>8%</td></tr> <tr><td>Rarely</td><td>7%</td></tr> <tr><td>Never</td><td>0%</td></tr> </table>	Frequency	Percentage	Always	58%	Often	27%	Occasionally	8%	Rarely	7%	Never	0%
Frequency	Percentage														
Always	58%														
Often	27%														
Occasionally	8%														
Rarely	7%														
Never	0%														
2	How would you rate your overall awareness of cybersecurity threats?	In response of this question 27% of the respondent were very high, 23% were high, 30% were moderate, 13% were low and 7% were very low about it.	<p>How would you rate your overall awareness of cybersecurity threats?</p>  <table border="1"> <tr><th>Rating</th><th>Percentage</th></tr> <tr><td>Very High</td><td>27%</td></tr> <tr><td>High</td><td>23%</td></tr> <tr><td>Moderate</td><td>30%</td></tr> <tr><td>Low</td><td>13%</td></tr> <tr><td>Very Low</td><td>7%</td></tr> </table>	Rating	Percentage	Very High	27%	High	23%	Moderate	30%	Low	13%	Very Low	7%
Rating	Percentage														
Very High	27%														
High	23%														
Moderate	30%														
Low	13%														
Very Low	7%														
3	Have you ever been a victim of a cyber-attack or online scam?	In response of this question 37% of the respondent were victim and 63% were not.	<p>Have you ever been a victim of a cyber-attack or online scam?</p>  <table border="1"> <tr><th>Response</th><th>Percentage</th></tr> <tr><td>Yes</td><td>37%</td></tr> <tr><td>No</td><td>63%</td></tr> </table>	Response	Percentage	Yes	37%	No	63%						
Response	Percentage														
Yes	37%														
No	63%														
4	Are you familiar with the term "Phishing"?	In response of this question 51% of the respondent were familiar and 49% were not.	<p>Are you familiar with the term "Phishing"?</p>  <table border="1"> <tr><th>Response</th><th>Percentage</th></tr> <tr><td>Yes</td><td>51%</td></tr> <tr><td>No</td><td>49%</td></tr> </table>	Response	Percentage	Yes	51%	No	49%						
Response	Percentage														
Yes	51%														
No	49%														
5	How often do you change your passwords for online accounts?	In response of this question 74% of the respondent were strongly agree, 26% were agree about it.	<p>How often do you change your passwords for online accounts?</p>  <table border="1"> <tr><th>Frequency</th><th>Percentage</th></tr> <tr><td>Regularly</td><td>18%</td></tr> <tr><td>Occasionally</td><td>22%</td></tr> <tr><td>Rarely</td><td>49%</td></tr> <tr><td>Never</td><td>11%</td></tr> </table>	Frequency	Percentage	Regularly	18%	Occasionally	22%	Rarely	49%	Never	11%		
Frequency	Percentage														
Regularly	18%														
Occasionally	22%														
Rarely	49%														
Never	11%														

6	Do you use unique passwords for different online accounts?	In response of this question 26% of the respondent were Always, 37% were sometimes, 28% were rarely use and 9% were never use.	<p>Do you use unique passwords for different online accounts?</p>  <ul style="list-style-type: none"> Always Sometimes Rarely Never
7	Do you keep passwords consist of uppercase, numbers, and special characters?	In response of this question 57% of the respondent were keep, and 43% were not.	<p>Do you keep passwords consist of uppercase, numbers, and special characters?</p>  <ul style="list-style-type: none"> Yes No
8	Do you use Multi factor Authentication?	In response of this question 36% of the respondent uses, and 64% were not.	<p>Do you use Multi factor Authentication?</p>  <ul style="list-style-type: none"> Yes No
9	Do you think Pirated software harm your computer?	In response of this question 56% of the respondent were agree and 44% were not about it.	<p>Do you think Pirated software harm your computer?</p>  <ul style="list-style-type: none"> Yes No
10	Do you think that the laws in effect are able to control cyber criminals?	In response of this question 11% of the respondent were strongly agree, 14% were agree, 21% were neutral and 23% were disagree and 31 were strongly disagree about it.	<p>Do you think that the laws in effect are able to control cyber criminals?</p>  <ul style="list-style-type: none"> Strongly Agree Agree Neutral Disagree Strongly Disagree



5. Preventive Measures against Cyber Attacks

The suggested steps aim to enhance cybersecurity awareness among college students, recognizing their heightened vulnerability. These measures are designed to effectively mitigate the risk of cyber-attacks.

- **Password Policy:**

It is recommended to always change your passwords for online accounts time to time and choose strong and complex passwords that includes a mix letters, numbers, and special characters to create a mental image or an acronym that is easy for you to remember. Avoid using easily guessable information like birthdates or names and also avoid to write down on sticky notes. Don't use unique passwords for different online accounts.

- **Turn on Multifactor Authentication:**

Integrate multifactor authentication on your accounts whenever feasible to introduce an additional level of security. This additional measure becomes crucial in the case if your password is leaked, this will make significantly strengthening the overall security of your account.

- **Install protective software:**

Configure protective software to routinely scan your files and regularly update virus definitions. Ensure that operating systems, software applications, and antivirus programs are consistently up to date, as numerous cyber-attacks capitalize on known vulnerabilities in outdated software.

- **Control access to your machine:**

The physical safeguarding of your device is equally crucial as its technical security. Avoid leaving your computer unattended or logged on in unsecured environments, particularly in public places. Always sign out of your account on the computer system, and monitor the individuals who access your system.

- **Use email and the Internet safely:**

Ignore unsolicited emails, and exercise caution when dealing with attachments, links and forms in emails originating from untrusted sources or those that appear suspicious, or which seem "phishy." Avoid untrustworthy (often free) downloads from freeware or shareware sites. Think before you click. More than 90% of successful cyber-attacks commence with a phishing email.

- **Use secure connections:**

Set up systems and applications with a focus on security in mind. When connected to the Internet, your data can be vulnerable while in transit. Use remote connectivity and secure file transfer options when off campus. Disable unnecessary services, change default passwords, and appropriately configure security settings to enhance protection.

- **Regular Backups:**

Ensure that you consistently verify the necessity of having a backup for your work and confidential files stored in a secure location. If the attack happens, you should not fall into data loss. Data loss not just affects financially but also affects the reputation.

- **Implement Network Segmentation:**

Divide networks into segments to restrict unauthorized access, limiting the potential damage of a cyber-attack.

- **Use desktop firewalls:**

Both Macintosh and Windows computers come equipped with built-in desktop firewalls as essential components of their operating systems. When configured correctly, these firewalls serve to safeguard your computer files, preventing unauthorized scanning.

- **Clean Cookies and Cache Memory:**

When we utilize the internet, cookies and cache memory are generated, these are created to save time while opening any web page which was opened before. But these are highly unsafe as these make our PC's prone to virus and hacking. Therefore, it is strongly advised to regularly clear this memory for enhanced security.

- **Most importantly, keep yourself stay informed:**

Keep update yourself with the most recent advancements in Windows, Macintosh, Linux, and UNIX systems. Ensure you consistently remain up-to-date with the latest information. Collaborate with Security Experts, take consultation in cybersecurity and remain updated on the most recent threats and best practices in security.

- **Familiarity with present-day threats:**

It is essential to have awareness of cyber-attacks to defend against particular cyber threats such as phishing, malware, ransomware, Denial-of-Service, spoofing, and more.

- **Ensure the security of your device:**

In the event of your mobile device being lost or stolen, there is a potential risk of unauthorized access to your information, financial resources, and personal data, including identity theft. Enhance the security of your devices by implementing measures such as setting up a password, gesture, or fingerprint for unlocking, configuring the device to demand a password before installing applications, maintaining Bluetooth in hidden mode when not in use, and disabling automatic connection to networks.

5. Conclusion

A broad subject that is growing more significant due to the world's increasing network connectivity is computer security against cybercrime. In this paper, systematic study was conducted, to evaluate the level of cybersecurity awareness among college students from diverse disciplines. Recognizing that cybersecurity awareness is crucial and an ongoing process demanding continual attentiveness. the study proposes a combination of measures rather than relying on a single solution for complete protection against cyber threats. While no method can ensure absolute security, the implementation of the suggested measures can substantially reduce the vulnerability to cyber-attacks. By adopting these measures, college students can receive valuable assistance in safeguarding against cyber theft and gaining awareness of various security tactics.

References

1. Abomhara, M., & Kjøien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.
2. Alexei, L. A. (2021). Network security threats to higher education institutions. In *Central and Eastern European eDem and eGov Days* (pp. 323-333).
3. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, 45, 3171-3189.
4. Reddy, G. N., & Reddy, G. J. (2014). A study of cyber security challenges and its emerging trends on latest technologies. *arXiv preprint arXiv:1402.1842*.
5. Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education

- institutions. *Information*, 13(4), 192.
6. Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015, November). An investigation on cyber security threats and security models. In 2015 IEEE 2nd international conference on cyber security and cloud computing (pp. 307-311). IEEE.
 7. Chivukula, R., Lakshmi, T. J., Kandula, L. R. R., & Alla, K. (2021, November). A Study of Cyber Security Issues and Challenges. In 2021 IEEE Bombay Section Signature Conference (IBSSC) (pp. 1-5). IEEE.
 8. Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, 13(4), 192.
 9. Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, 27(7-8), 241- 253.
 10. https://www.researchgate.net/publication/347278652_Cyber_security_awareness_among_students_and_faculty_members_in_a_Sudanese_college
 11. Gordon S., Ford, R.: *Cyberterrorism? In: Cyberterrorism. The International Library of Essays in Terrorism*, Alan O'Day, Ashgate, ISBN 0 7546 2426 9 (2004)
 12. Krone T.: *High tech crime brief*. Australian Institute of Criminology, Canberra, Australia, ISSN 1832–3413 (2005).
 13. Harrell, C. R., Patton, M., Chen, H., & Samtani, S. (2018, November). Vulnerability assessment, remediation, and automated reporting: Case studies of higher education institutions. In 2018 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 148-153). IEEE.
 14. Sun, W., & Wu, L. (2019, December). Research on network and information security in Colleges and Universities. In 2019 International Conference on Information Technology and Computer Application (ITCA) (pp. 292-295). IEEE.
 15. Reddy, G. N., & Reddy, G. J. (2014). A study of cyber security challenges and its emerging trends on latest technologies. arXiv preprint arXiv:1402.1842.