https://doi.org/10.59862/k7m2x9q4r8/03

Chapter 3

Cybersecurity in the Academic Environment: Scientific Institutions as Targets of Cyber-attacks

ANDRII DAVYDIUK
G.E. Pukhov Institute for Modelling in Energy Engineering
at National Academy of Sciences of Ukraine
ORCID 0000-0003-1238-2598

Abstract: Scientific institutions and research facilities are increasingly becoming targets of cyberattacks. The consequences of such attacks can include data theft and integrity breaches, loss of intellectual property, reputational damage, and threats to national security. This study proposes to examine scientific institutions as multi-layered targets for malicious actors who may have espionage and destructive motives. Key sub-targets that are frequently attacked include students, faculty, other staff, databases, neural network-based systems and artificial intelligence, as well as other IT systems. This approach allows for the formation of a structured cybersecurity profile of the research institution. By "profile," proposed to mean a set of typical characteristics of scientific institutions in the context of cybersecurity. This research aims to develop a cybersecurity profile for scientific institutions that includes a classification of typical threats, a list of potential attack targets, and possible risks. A separate analysis of case studies based on real examples is also conducted. This profile will not only help identify the main vulnerabilities of the institution but will also serve as a practical tool for enhancing cybersecurity within the academic environment. Specifically, this section attempts to summarize knowledge about cyber threats in the academic sector and propose concrete methods for protecting critical data and research resources.

The relevance of this research is confirmed by real threats, including espionage by China against the United States and other countries.[1] Moreover, the involvement of scientific institutions as subjects of cyberattacks2 also represents a distinct threat in cyberspace, which will have a unique profile. A striking example of the importance of cybersecurity in the scientific sector is the war in Ukraine, where scientific institutions are actively targeted by adversaries. Data about research projects in the fields of security and defense, energy, etc., as well as personnel lists of military institutes, are valuable to adversaries. Such information allows for the assessment of the strength and capabilities of the Ukrainian army and is used to prepare battle strategies. This underscores the strategic significance of information and cybersecurity for scientific institutions in military conflicts. The proposed profile can be used to develop effective cybersecurity measures aimed at protecting critical data and reducing risks in the academic environment. At the same time, it also promotes collaboration between scientific institutions and governmental bodies in the field of cybersecurity for data and protection method exchange, including in an international context. This approach is particularly relevant for countries experiencing military conflicts or facing intense cyber threats from foreign states.

Keywords: cyberattacks, cybersecurity, scientific institutions, intellectual property, national security

Scientific and educational institutions are an important component of the state. The training of specialists, conducting research, attracting foreign investments depends on them. Ensuring cyber security and information security is an integral part of the functioning of any scientific institution. Vulnerabilities in the education sector go far beyond immediate disruption, but can potentially compromise research integrity, data privacy, and the financial stability of these outstanding institutions.

Let's consider in more detail why scientific institutions become the targets of cyber-attacks. One of the reasons may be an offended student who, in his or her opinion, received a low grade and wants to take revenge on the educa-

[1] "Survey of Chinese Espionage in the United States Since 2000," Center for Strategic and International Studies, accessed November 21, 2024, https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000.

[2] Dakota Cary, "Academics, AI, and APTs," Center for Security and Emerging Technology, March 2021, https://cset.georgetown.edu/publication/academics-ai-and-apts/.

tional institution. Another motive on the part of the student may be to sabotage the educational process due to unwillingness to pass the test or change the assessment results. However, it is not only students that pose a threat. An educational institution can become a victim of a cyber-attack due to unfair competition. Obtaining grants is always a competition and reputational damage due to missed deadlines can be the reason for refusal of grants. One cannot reject the natural competition among scientists for the primacy of discovery and scientific glory. All these factors can be attributed to internal threats, but in addition, there are also external ones.

External threats include primarily espionage, theft of ideas, and slowing down of research. A vivid example of such a hunt for information was the Cold War.[3] Another example is attacks on scientific institutions conducting COVID-19 research that were a significant cyber threat during the pandemic. Hacker groups such as APT29 (linked to Russia) have attempted to steal information related to the development of vaccines against COVID-19. The attackers used special malware ("WellMess" and "WellMail") as well as known software vulnerabilities to gain access to the networks of institutions in Canada, the United States and the United Kingdom.[4] [5] During the Russian-Ukrainian war, the object of the enemy's interest, among others, are military educational institutions that prepare future officers for the Ministry of Defence, the armed forces, and other military formations. For the enemy, they are a source of data on the number of specialists, their level of training, material base, individual cadets and officers who can be swayed to their side. All these data enable the enemy to more effectively prepare for war and develop attack tactics. In addition, departmental institutes of the defense sector can be exposed to cyber-attacks as

[3] John L. Gaddis, "Intelligence, Espionage, and Cold War Origins," Diplomatic History 13, no. 2 (1989), 191–212.

[4] Cybersecurity and Infrastructure Security Agency, "COVID-19 Cyber Threats (Update)", August 30, 2020, https://www.cisa.gov/sites/default/files/publications/202008131030_COVID-19%20Cyber%20Threats%20Update_TLP_WHITE.pdf.

[5] Adam Bannister, "Bad Education: Universities Struggle to Defend Against Surging Cyber-Attacks During the Coronavirus Pandemic," The Daily Swig | Cybersecurity News and Views, February 23, 2021, https://portswigger.net/daily-swig/bad-education-universities-struggle-to-defend-against-surging-cyber-attacks-during-coronavirus-pandemic.

part of the department that the adversary wants to damage. For example, DDoS attacks on their websites, disruption of training processes, etc. In the spring of 2020, the number of DDoS (Distributed Denial of Service) attacks in the education sector increased by 350%.[6] The percentage increase of such attacks on the education sector in 2021 was 102%. Such attacks disrupt critical operations such as class scheduling, assignment, and the admissions process.[7] For example, the hacktivist group Anonymous Sudan launched a DDoS attack against some of the UK's top universities. This attack caused significant damage and disruption. Because of this attack, the Computing Service of the University of Cambridge Clinical School had to experience unstable internet access. Shedding light on the interconnected nature of cyber risks at universities, the network issue was just one part of a larger attack on the Jane Network. Jane's network unites several universities.[8] But there were also other types of attacks, for example, you can cite an incident at the University of Minnesota, when in 2021, cybercriminals hacked into a database containing student financial applications. The attackers gained access to personal information, including names, addresses, social security numbers and even passport information. The leak was only discovered in 2023, when the stolen data began to appear online.[9] In 2023, Indiana University was found to have stored student survey data that included sensitive information (sexual orientation, race, etc.) on unsecured cloud storage. This led to the leak of almost 250,000 records.[10]

---

[6] "DDoS Attacks Against Educational Resources Increased by More Than 350%, Says Kaspersky," *Intelligent CIO* https://www.intelligentcio.com/me/2020/09/15/ddos-attacks-against-educational-resources-increased-by-more-than-350-says-kaspersky/.

[7] NETSCOUT Systems, Inc., "Bad Actors Innovate, Extort and Launch 9.7M DDoS Attacks in 2021 According to the Latest NETSCOUT Threat Intelligence Report," March 22, 2022, https://ir.netscout.com/investors/press-releases/press-release-details/2022/Bad-Actors-Innovate-Extort-and-Launch-9.7M-DDoS-Attacks-in-2021-According-to-the-Latest-NETSCOUT-Threat-Intelligence-Report/default.aspx.

[8] James Coker, "Top UK Universities Recovering Following Targeted DDoS Attack," Infosecurity Magazine, February 20, 2024, https://www.infosecurity-magazine.com/news/universities-recovering-ddos-attack/.

[9] University of Minnesota System, "Data Incident," University of Minnesota System, accessed November 24, 2024,https://system.umn.edu/data-incident.

[10] "IU Reports Records Exposed in Data Breach Are Public Domain," Indiana Public Media, July 13, 2023, https://indianapublicmedia.org/news/indiana-university-suffers-second-data-leak-this-year.php.

Exploitation of vulnerable file transfer software (MOVEit) allowed cybercriminals to gain access to student and employee data at the University of Georgia, including social security numbers, contact information, and payroll information.[11] Lincoln College was forced to close due to a massive ransomware attack in 2021. The attack disrupted access to data and complicated the process of recruiting students, which caused significant financial losses and became fatal for the institution.[12] In June 2022, the University of Pisa fell victim to the BlackCat ransomware group, which hijacked the university's IT system before demanding a whopping $4.5 million ransom, making it one of the largest ransom demands of 2022.[13] Cyberattacks can disrupt and disable critical systems that support student registration portals, learning systems, and financial transaction systems. This may lead to interruption of educational activities and administration work. For example, in 2023 there was a large-scale attack on "Neptune," an online portal for students and teachers used by the University of Pecs and other universities in Hungary. The attack occurred during university exams and caused serious service disruptions. The universities had to face the system failure for two months. Academic evaluations were delayed and administrative work was distracted due to the temporary shutdown of the system. The shutdown also proved that key academic systems are not immune to cyberattacks.[14]

A separate aspect of the information security of educational institutions is the physical security of their IT systems, as there have already been cases of kinetic attacks on educational institutions. Specifically, on September 3, 2024, two Russian missiles hit a branch of the Military Institute

[11] University System of Georgia, "Notice of Data Breach," University System of Georgia, April 15, 2024, https://www.usg.edu/news/release/notice_of_data_breach.

[12] Graham Cluley, "US College Set to Permanently Close After 157 Years, Following Ransomware Attack," Hot for Security, May 11, 2022, https://www.bitdefender.com/en-us/blog/hotforsecurity/us-college-set-to-permanently-close-after-157-years-following-ransomware-attack.

[13] Scott Zelko, "A Recap of Recent Cybersecurity Incidents at Universities," Schellman Compliance, November 14, 2023, https://www.schellman.com/blog/cybersecurity/cybersecurity-incidents-at-universities-2023.

[14] Fares Barauj, "Importance of Cybersecurity in Educational Institutions," July 2024, https://www.researchgate.net/publication/382495313_Importance_of_Cybersecurity_in_Educational_Institutions.

of Telecommunications and Information Technologies and a nearby hospital in Poltava, Ukraine, killing at least 59 and injuring at least 328.[15]

It is worth noting that the targets of cyber-attacks are not only educational institutions, but also teachers and researchers working in them. Many of the teachers take their work home and work from their own computer, so the personal device is a data carrier for research and may have access parameters to the resources of the educational institution. In addition, scientists who are teachers can hold positions in production or take part in public administration. With this in mind, cyber security in academic institutions should include protection of IT systems used for research and cyber hygiene work for staff, and cyber security in the scientific sphere becomes a matter of national security. Overall, the record growth in attacks in the third quarter of 2024 saw an average of 1,876 cyberattacks per organization, a 75% increase over the same period in 2023 and a 15% increase over the previous quarter. And the education/research sector was the most attacked with 3,828 attacks per week, followed by the government/military and healthcare sectors with 2,553 and 2,434 attacks respectively (see Figure 1).[16]

Of course, information security is also affected by the working conditions of scientists. This includes the quality of hardware and software for cyber protection, the presence of information security policies in place, the awareness of personnel about cyber security threats and their actions in the event of a cyber-attack. Unfortunately, not all educational institutions can afford expensive hardware and software to protect their own systems, provide adequate remuneration for an information security specialist, or open such a position. Because of this, many senior teachers, due to their low level of awareness in working with digital technologies, become victims of phishing, malware, extortionists, and data encryptors. The University of Arkansas is a real-life example of phishing in higher education. The university witnessed

[15] RCB-Ukraine, "Russia Strikes Educational Institution With Ballistic Missiles in Poltava: 41 Killed, 180 Wounded," RBC-Ukraine, September 3, 2024, https://newsukraine.rbc.ua/news/russia-strikes-educational-institution-with-1725366089.html.

[16] Check Point Team, "A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide," Check Point Research Blog, October 25, 2024, https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/.

Figure 1. Comparison of the number of cyber-attacks per week by sector

a noticeable increase in the number of phishing emails. Faculty, staff, and students were the subjects of these emails. The university said the attacks resulted in many members becoming victims and accounts being compromised. The importance of being vigilant and educated about cyber security is highlighted by the rise in phishing attacks, especially during downtime. Several methods have been implemented by the University of Arkansas to overcome the dangers of this threat.[17]

The presence of such problems requires the development of a systematic approach to information protection in scientific institutions. Thus, it is expedient to classify scientific institutions. This classification may differ from general practice, in particular by subordination, specialties, etc. Classification in the field of information security is designed to identify potentially attractive scientific institutions for the enemy, and to identify critical processes, research, and possible threats in them. Appropriate measures in such a clas-

[17] Fares Barauj, "Importance of Cybersecurity in Educational Institutions," July 2024 July 2024 https://www.researchgate.net/publication/382495313_Importance_of_Cybersecurity_in_Educational_Institutions.

sification would include dividing institutions into military and civilian categories; considering whether they conduct research in security, defense, national security, or critical infrastructure; identifying any international collaborations; and noting whether their staff includes representatives from government bodies, the security and defense sector, or related industries. Such a classification will make it possible to determine the specifics of the work of such institutions, in particular, work with information with limited access, requirements for personnel, and requirements for IT systems of such institutions. After such a basic classification, it will be possible to proceed to the prioritization of scientific institutions according to the impact of their activities on national security. By impact, it will be possible to qualitatively distinguish critical and important for national security.

At this stage, the question arises of developing requirements and evaluation methods (self-evaluation) of educational institutions of different categories in accordance with the classification proposed above. The requirements should be based on the profile of the institution according to the classification and take into account the assessment of the disruption of research processes (damage) or the leakage of sensitive research data. For example, military institutions should focus on protecting the personal data of cadets and employees, limiting access to information about the material base and the content of educational programs. The assessment (self-assessment) should include an assessment of the state of cyber protection of the IT infrastructure and the available means for this. Availability of security policies and staff awareness of cyber hygiene rules. This will enable effective planning to build their cyber security capabilities.

A separate aspect of cyber security is the possibility of the adversary using scientific institutions for cyber-attacks. Poorly protected servers, desktops in computer science classes, and clusters can be used for cyber-attacks if an attacker has unauthorized access. The use of such concentrated multi-user resources enables the attacker to increase his or her own anonymity and complicate the task of rapid localization for the defense side.

Therefore, scientific institutions need a systematic approach to cyber protection. The development and implementation of such an approach requires

educational and scientific institutions to develop their own capacities and the attraction of resources. Quantum computing opens up new possibilities for attacks. Quantum computer algorithms can break modern encryption systems, putting even the most protected institutions at risk. In addition, the aggravation of geopolitical tensions at the present time increases the risks of cyberespionage, which is especially dangerous for scientific institutions with international projects. Thus, the issue of cyber security, in addition to national security, should be a matter of cyber diplomacy and diplomacy in science. At the same time, international collaboration around the problems of cyber and information security can significantly draw attention to this problem and facilitate processes in the government to develop relevant regulatory documents for the institutionalization of these processes. It is worth noting that information protection processes should not create a negative impact on the implementation of open science and the reproduction of science.

Personal

1. Use two-factor authentication.[18]
2. Remember to protect your hardware, such as setting BIOS/UEFI passwords, locking your computer when you're away, using secure workstations.
3. Use licensed/legalized operating systems and other software products, and systematically update them in a timely manner.
4. Use antivirus software with heuristic analysis technology.
5. Use a software firewall and standard anti-malware tools.
6. Back up your data regularly, store backups on external media (SSD, HDD, etc.), and set up system restore.
7. Cloud services that use synchronization (for example, Dropbox, OneDrive, SharePoint, and Google Drive) should not be used as the only environment for saving backup copies. The disadvantage of these systems is that they can automatically synchronize immediately after infection of the files, and it is also possible to lose backup copies.

[18] CERT-UA, Фактор кібербезпеки, April 1, 2024, https://cert.gov.ua/recommendation/6278274.

Note. For the most part, encrypted files cannot be decrypted by anyone. Don't waste your time or money on services that promise to do this. In some cases, cyber security experts can provide programs that can decrypt files due to malware flaws. We recommend not using programs to decrypt data from unverified sources.

8. Do not connect flash drives and external drives, do not insert CDs and DVDs, etc., into your computer unless you fully trust their source. There are techniques for hacking your computer even before you open the file on the flash drive and long before your antivirus scans it. If you found a device inside the office or on the street, received it in the mail or with a delivery, or a stranger gave it to you with a request to print a document, or simply open it and check its contents, there is a good chance that the device is dangerous.
9. Only trust your own devices and be careful with devices you receive from other people for work or other purposes.
10. When connecting devices, ensure that they are automatically checked for malware.
11. Disable automatic startup of removable media (protection from autorun.inf).
12. Do not store authentication data in easily accessible places (for example, on the desktop). Use special software tools (for example, KeePass) to store passwords. Use strong passwords, in particular, those that: contain at least eight characters; contain letters, numbers and special characters; do not contain personalized information (date of birth, phone numbers, numbers and series of documents, vehicles, bank card, registration address, etc.); not used in any other accounts.
13. Avoid using internet banking, electronic payment systems, entering authentication data when accessing the internet through public (unsecured) wireless networks (in cafes, bars, airports, and other public places).
14. Be especially careful when opening email attachments from unknown persons. Today, the most relevant means of distributing malware is email. When working with email, you should check the extensions of attached files and not open files even with safe extensions. Do not follow

unknown links or download files with potentially dangerous extensions (e.g.: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js, etc.) and even safe ones (e.g.: .docx, .zip, .pdf), because vulnerabilities, macros, and other dangers may be used. Pay attention to the email name: even if it seems legitimate, you still need to verify (by phone or otherwise) that the person actually sent you the message with the attachment.

15. Sometimes, especially under time pressure, it can be difficult to distinguish malicious files from legitimate files. Use the service VirusTotal[19] to check suspicious files by simultaneously scanning them with more than 50 antiviruses. This is much more efficient than scanning files with an antivirus offline, but consider the fact that by uploading files to VirusTotal, you are giving access to it to a third party. We draw your attention to the fact that even if the check on VirusTotal did not give a result, this does not exclude the fact that the file may be malicious.
16. Think twice before opening attachments.
17. When using internet resources (internet banking, social networks, messaging systems, news, online games), do not open suspicious links (URLs), especially those that point to websites that you do not normally visit.
18. Be alert to internet scams. The most common means of deception on the internet is phishing. Pay special attention to the domain name of the internet resource that asks for authentication data before clicking on the link: attackers can mask the domain name to make it look familiar (facelook.com, gooogle.com, etc.). Otherwise, there is a high probability of going to a phishing page, which is identical to the real one, and "giving away" your own authentication data.
19. If you need to enter credentials, make sure you're using a secure HTTPS connection, and check the website's SSL certificate to make sure it hasn't been cloned or spoofed.
20. Malicious URLs can be encoded in the form of QR codes and/or printed on paper, including in the form of shortened URLs generated by

[19] VirusTotal, https://www.virustotal.com/gui/home/upload.

special services such as tinyurl.com, bit.ly, ow.ly, etc. Do not enter these links into a browser or scan QR codes with your smartphone if you are not sure of their content and origin.

21. Use VirusTotal[20] to check for suspicious links in the same way as for scanning files.
22. Be careful about pop-ups and messages in your browser, apps, operating system, and mobile device. Always read the contents of these windows and do not "approve" or "accept" anything hastily.
23. When using remote access, it is necessary to limit access using "white list" (IP whitelisting).
24. Set a limit on the number of incorrect logins/passwords. Regularly review the login logs, task scheduler, and autostart for unauthorized activity.
25. Stay up-to-date on new cyber threats and respond quickly to new challenges.[21]

For Institutions

1. Advise employees to conduct a potential risk assessment, such as studying possible attack scenarios that may target their institution or position.
2. Conduct training for employees on protection against social engineering methods (in particular, telephone attacks, blackmail, manipulation).
3. Emphasize the importance of paying attention to unusual events—for example, sudden changes in settings, the appearance of unusual programs or files.
4. Ensure availability of system administrators (security administrators) at the object(s).
5. Ensure monitoring of information security events.
6. Identify responsible persons for responding to cyber incidents during interaction with relevant government agencies.

[20] VirusTotal, https://www.virustotal.com/gui/home/upload.

[21] CERT-UA, Основні правила кібергігієни, December 13, 2018, https://cert.gov.ua/recommendation/31.

7. Form a team of IT (information security) specialists to respond to computer emergency events.
8. Create an incident response plan, including attack recovery scenarios, and train employees on what to do in such situations.
9. Regularly audit all devices, software, and access to ensure you are in control of your infrastructure.
10. Conduct training with all employees who have access to information systems on compliance with information security policies (cyber hygiene rules) and pay attention to the use of internet resources and email, responding to phishing messages.
11. Back up critical (important) information resources and store their backup copies in separate data repositories.
12. Update operating systems and software to the latest versions.
13. Enable all possible event logging options and ensure their storage on a separate disk storage.
14. Check and enable anti-virus protection and update the anti-virus software signature database.
15. Create policies that will only allow downloading files of the types that should be received (for example, prohibit receiving or transferring .EXE files).
16. Block websites that are harmful.
17. Check suspicious files by antivirus programs, in the absence of a licensed antivirus, we recommend using the free VirusTotal or Cuckoo sandbox service.
18. If this is relevant for the institution (for example, in the case of public services), implement a solution to prevent DDoS attacks.
19. Use signatures to block known malicious code.
20. Use mail filtering (combined with spam filtering) that can block malicious email messages and delete suspicious attachments.
21. Use tools that block known malicious websites on relevant lists.
22. Use tools with information security features that can scan data content for known malware.

23. When using remote access, only allow connection to specified users using "white list" (IP whitelisting).[22]
24. For internal information exchange, it is recommended to use solutions with end-to-end encryption.
25. Carry out self-scanning for vulnerabilities of information resources posted on the internet or contact the relevant state body.
26. Eliminate vulnerabilities in information systems.
27. Disable remote access to information systems or review the circle of employees who are granted the right to remote access to information systems during the holidays, and implement maximum restrictions (filtering by IR, protocols, access time, users, etc.).
28. Implement the principle of least privilege (Least Privilege) for all employees and systems.
29. Provide security policies for employees' mobile devices (e.g., data encryption, mandatory use of passwords, ability to remotely delete data).
30. If the institution uses the API, configure protection against unauthorized access, for example, using OAuth 2.0 or other modern standards.
31. It is also recommended to add a separate section to protect IoT devices (if used) and avoid using equipment that does not support regular firmware updates.
32. Only use securely protected remote access methods and protocols for the administration of information systems and resources that have an appropriate level of encryption.
33. Use strong passwords and set up multi-factor authentication.[23]
34. Block access from the internet to versions of software and information systems that are no longer supported by the manufacturer or the functioning of which is not critical.
35. Turn off all services and information systems that will not be used.[24]

[22] CERT-UA, Зага++льні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення, July 21, 2020, https://cert.gov.ua/recommendation/2502.
[23] National Cyber Security Centre, Top Tips for Staying Secure Online, December 21, 2021, https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers.
[24] SCPC-UA, Recommendations from the State Cyber Protection Center, January 24, 2022, https://scpc.gov.ua/uk/recommendations/129.

36. Constantly monitor the versions of the operating system, content management system (CMS), package manager, frameworks or other software that ensure the operation of the web resource, and regularly update them. At the same time, it is better to use only the "LTS" version.
37. The use of the HTTPS protocol guarantees the integrity and confidentiality of interaction with the server and protects user data when transmitted over the internet. The certificate must be issued by a certification authority.
38. Use the latest version of TLS (SSL has flaws and vulnerabilities and is not acceptable for secure communication).
39. It is a good practice to configure the HSTS (HTTP Strict Transport Security) mechanism to force HTTPS to be used, even when clicking on links that explicitly specify the HTTP protocol.
40. If the web resource does not have its own logging system, monitor the log files of the web server (access.log). In the log files, pay attention to POST requests and the server's response code to them.
41. Pay special attention to POST requests to pages that should not receive any data, or that should not exist at all. This may indicate unauthorized actions with the web resource.
42. Usually, after hacking web resources, attackers leave backdoors (webshells) on the server for remote access to the site's server. Periodically check the web application directories for such backdoors. For this purpose, it is possible to use special scripts or simply check the presence of new files in the directories. The detection of files created by third parties will indicate the hacking of the web resource and provide opportunities for further actions to find vulnerabilities that were used.[25]
43. Configure file and directory permissions. Distribute access rights to files on the server and individual sections of the site according to user tasks. Distinguish between the location of scripts and programs, data intended for reading only, and data intended for modification by visitors.

[25] CERT-UA, Рекомендації з самостійного пошуку та ліквідації веб-шеллів, https://cert.gov.ua/files/pdf/CUA-14-06R.pdf.

44. Hacking a website starts with gathering information about the server. Hiding versions of the used software is one of the elements of ensuring the security of the web server. Knowing the versions of these programs can facilitate the attacker's task of finding vulnerabilities known for this version and, as a result, in achieving the main goal—penetration. Therefore, it is necessary to hide service pages (e.g., phpinfo.php, temp.php, test.php.) and service information displayed in error messages.
45. Turn off unnecessary services. Block unused ports, configure a firewall, and/or Web Application Firewall (WAF).
46. Restrict access to the administrator panel from the internet and public networks.
47. Change your site and server access passwords regularly.
48. Use secure server access methods for file transfer and management (SFTP, SSH, etc.).
49. Configure input filtering in web forms.
50. Back up your site and database (if any) regularly.
51. It is quite common to observe the location of several unrelated web resources on one virtual machine. For example, a website and an old version of the website, or a new test version. The old version is not supported and has old vulnerabilities, the test version is incomplete and also vulnerable, while they are accessible from the internet. Due to the vulnerabilities of these web resources, attackers gain unauthorized access to the main web resource.[26]
52. Configure MS Office security settings,[27] CorelDRAW, Notepad++.
53. Take safety measures for organizing remote work.[28]
54. Foster partnerships between academic institutions, government and international organizations to improve information sharing, establish

[26] CERT-UA, "Рекомендації CERT-UA з безпеки вебресурсів." January 27, 2020, https://cert.gov.ua/recommendation/19.

[27] CERT-UA, "Рекомендації CERT-UA з налаштувань MS Office", https://cert.gov.ua/files/pdf/Recommendations-MSOffice.pdf

[28] CERT-UA, "Рекомендації щодо організації віддаленої роботи", April 4, 2021, https://cert.gov.ua/recommendation/11388

best practices, and develop regulatory frameworks. Maintain a balance between cybersecurity and the principles of open science, ensuring the accessibility of research and the protection of sensitive data.

55. Address budget constraints by implementing scalable cyber defense solutions and sharing resources across agencies. Increase the stability of institutions by developing internal expertise and attracting support from the state.
56. For scientific institutions engaged in development in the field of security and defense, use legending and additional security measures.

Bibliography

Center for Strategic and International Studies. "Survey of Chinese Espionage in the United States Since 2000." csis.org, March 2023. https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000.

Cary, Dakota. "Academics, AI, and APTs How Six Advanced Persistent Threat-Connected Chinese Universities Are Advancing AI Research". cset.georgetown.edu, March 2021. https://cset.georgetown.edu/publication/academics-ai-and-apts/.

Gaddis, John L. "Intelligence, Espionage, and Cold War Origins." Diplomatic History 13, no. 2 (1989): 191–212.

"COVID-19 Cyber Threats (Update)". cisa.gov, 13 August 2020. https://www.cisa.gov/sites/default/files/publications/202008131030_COVID-19%20Cyber%20Threats%20Update_TLP_WHITE.pdf.

Bannister, Adam. "Bad Education: Universities Struggle to Defend Against Surging Cyber-Attacks During Coronavirus Pandemic." The Daily Swig | Cybersecurity news and views, February 23, 2021. https://portswigger.net/daily-swig/bad-education-universities-struggle-to-defend-against-surging-cyber-attacks-during-coronavirus-pandemic.

Bowen, Mark. "DDoS Attacks Against Educational Resources Increased by More Than 350%, Says Kaspersky – Intelligent CIO Middle East." *Intelligent CIO*, September 15, 2020. https://www.intelligentcio.com/me/2020/09/15/ddos-attacks-against-educational-resources-increased-by-more-than-350-says-kaspersky/.

"Bad Actors Innovate, Extort and Launch 9.7M DDoS Attacks in 2021 According to the Latest NETSCOUT Threat Intelligence Report." ir.netscout.com, March 22, 2022. https://ir.netscout.com/investors/press-releases/press-release-details/2022/Bad-Actors-Innovate-Extort-and-Launch-9.7M-DDoS-Attacks-in-2021-According-to-the-Latest-NETSCOUT-Threat-Intelligence-Report/default.aspx.

Coker, James. "Top UK Universities Recovering Following Targeted DDoS Attack." Infosecurity Magazine, February 20, 2024. https://www.infosecurity-magazine.com/news/universities-recovering-ddos-attack/.

"Data Incident." University of Minnesota System. Дата звернення, July 29, 2025. https://system.umn.edu/data-incident.

"IU Reports Records Exposed in Data Breasch Are Public Domain." *Indiana Public Media*. July 13, 2023. https://indianapublicmedia.org/news/indiana-university-suffers-second-data-leak-this-year.php.

"Notice of Data Breach | Communications | University System of Georgia." University System of Georgia, April 14, 2024. https://www.usg.edu/news/release/notice_of_data_breach.

Cluley, Graham. "US College Set to Permanently Close After 157 Years, Following Ransomware Attack." Hot for Security, May 11, 2022. https://www.bitdefender.com/en-us/blog/hotforsecurity/us-college-set-to-permanently-close-after-157-years-following-ransomware-attack.

Zelko, Scott. "A Recap of Recent Cybersecurity Incidents at Universities." Schellman Compliance, November 14, 2023. https://www.schellman.com/blog/cybersecurity/cybersecurity-incidents-at-universities-2023.

Ibrahim, Fares. "Importance of Cybersecurity in Educational Institutions." July 2024. https://www.researchgate.net/publication/382495313_Importance_of_Cybersecurity_in_Educational_Institutions?channel=doi&linkId=66a0b0fe5919b66c9f683dbe&showFulltext=true.

Oleniak, Liliana. "Russia Strikes Educational Institution With Ballistic Missiles in Poltava: 41 Killed, 180 Wounded." RBC-Ukraine, March 9, 2024. https://newsukraine.rbc.ua/news/russia-strikes-educational-institution-with-1725366089.html.

"A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide." blog.checkpoint.com, October 18, 2024. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/.

"CERT-UA Фактор кібербезпеки." cert.gov.ua, April 1, 2024. https://cert.gov.ua/recommendation/6278274.

"VirusTotal." VirusTotal. Accessed July 29, 2025. https://www.virustotal.com/gui/home/upload.

"CERT-UA Основні правила кібергігієни." cert.gov.ua, December 13, 2018. https://cert.gov.ua/recommendation/31.

"CERT-UA Загальні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення." cert.gov.ua, July 21, 2020. https://cert.gov.ua/recommendation/2502.

"Managing Your Passwords." NCSC. Дата звернення July 29, 2025. https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers.

"Рекомендації державного центру кіберзахисту." scpc.gov.ua, January 24, 2022. https://scpc.gov.ua/uk/recommendations/129.

CERT-UA. Рекомендації з самостійного пошуку та ліквідації веб-шеллів. https://cert.gov.ua/files/pdf/CUA-14-06R.pdf.

"CERT-UA рекомендації CERT-UA з безпеки вебресурсів." cert.gov.ua, January 27, 2020. https://cert.gov.ua/recommendation/19.

CERT-UA. Рекомендації CERT-UA з налаштувань MS Office. https://cert.gov.ua/files/pdf/Recommendations-MSOffice.pdf.

CERT-UA. Рекомендації щодо організації віддаленої роботи. April 4, 2021. https://cert.gov.ua/recommendation/11388.