DOI: https://doi.org/10.31392/NZ-udu-164-2.2025.19
УДК 378.091.3:004]:004.6-049.65

Шимків Н. І.

ЗАСТОСУВАННЯ СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ В ОСВІТНЬОМУ ПРОЦЕСІ ПІДГОТОВКИ ФАХІВЦІВ ЦИФРОВИХ ТЕХНОЛОГІЙ

Стаття присвячена аналізу та практичному обґрунтуванню використання сучасного та актуального програмного забезпечення у підготовці фахівців з кібербезпеки в сфері цифрових технологій в умовах зростання кіберзагроз та збільшення впливу цифровізації на суспільство. Розглядається доцільність упровадження технологічних інструментів в освітній процес, що зумовлена потребою у формуванні практичних навичок реагування на інциденти, аналізу трафіку, виявлення вразливостей та моделювання реальних сценаріїв атак. Досліджено, що традиційні освітні методики вже не забезпечують достатнього рівня підготовки, оскільки сучасна кібербезпекова діяльність передбачає роботу зі складними мережевими інфраструктурами, цифровою криміналістикою, автоматизованим моніторингом та інструментами пентестингу.

Проведено аналіз основних типів програмного забезпечення, що застосовується у навчанні: середовища віртуального доступу (VirtualBox, VMware Workstation), платформи для симуляції та платформи-тренажери (TryHackMe, HackTheBox), інструменти аналізу мережевого трафіку (Wireshark), комплексне програмне забезпечення для тестування безпеки (Metasploit Framework), системи моніторингу та різнотипні журнали безпеки та моніторингу мережі (Splunk, ELK Stack). Для кожного з розглянутого прикладного програмного забезпечення подано рекомендації щодо використання їх на лабораторних заняттях, під час проведення практики, та можливість моделювання інцидентів.

Розкрито педагогічні і методичні властивості віртуальних середовищ, що дозволяють створювати повноцінні навчальні та симуляційні лабораторії та аналізувати функціонування реальних мереж та систем. Досліджено, що платформи типу CTF дозволяють розвинути навички етичного хакінгу, так званої кіберрозвідки (тестування на вразливості). Виділено особливість застосування прикладного програмного забезпечення Wireshark для мережевого аналізу та моніторингу мережі, що дає студентам можливість аналізувати та визначати різноманітні типи трафіку та ознаки та властивості кібератак. Metasploit Framework використовується, як один з найефективніших інструментів для демонстрації повноцінного тестування системи на проникнення, тоді як системи SIEM, зокрема Splunk та ELK, розглянуто як необхідні у формуванні компетентностей аналітика та фахівця.

У статті зроблено висновок, що повноцінне та всебічне застосування програмного забезпечення для захисту даних у процесі підготовки фахівців цифрових технологій підвищує ефективність професійної підготовки, забезпечує наближення процесу здобуття освіти до реальної практики та вмінням протистояти загрозам, формує поглиблене розуміння актуальних методів атак та способів їх виявлення та усунення. Подальший розвиток методики має ґрунтуватися на розширенні практичного застосування програмного забезпечення для імітації, введення автоматизованих процесів у проведення практичних занять та можливість виділення індивідуальних освітніх траєкторій, залежно від рівня підготовки здобувачів.

Ключові слова: *Педагогічні методи, освітній процес, практична підготовка, цифрові технології, підготовка фахівців, цифрова трансформація, захист даних, система підготовки, практичні вміння.*

Через безперервний та дуже швидкий розвиток цифрових технологій та їх впровадження у сучасний світ, а також у зв'язку із значним поширенням кіберзагроз неможливо переоцінити важливість якісної підготовки фахівців у галузі кібербезпеки. В умовах викликів гібридної війни, кібератак на критичну інфраструктуру та активного використання інформаційних технологій у всіх сферах діяльності виникає потреба в актуалізації та виділенню особливо ефективних інструментів навчання, що можуть забезпечити формування практичних умінь та навичок для сучасних здобувачів освіти у галузі професійної освіти. Одним із основних та необхідних складових сучасної підготовки є використання спеціалізованих прикладних засобів, які дозволяють створювати реальні сценарії атак та кіберзагроз, проводити поточний аналіз недоліків, здійснювати постійний контроль журналів безпеки та відпрацьовувати реагування на кіберзагрози. Тому поданий аналіз програмного забезпечення для освітнього процесу є актуальним завданням для оптимізації та осучаснення змісту навчання фахівців у сфері цифрових технологій.

Мета дослідження полягає у визначенні найбільш ефективних і поширених та актуальних програмних комплексів, що застосовуються для підготовки фахівців цифрових технологій пов'язаних із захистом даних, а також в аналізі їхніх функціональних можливостей, переліку переваг та недоліків використання їх у освітньому процесі.

Методи дослідження передбачають:

– аналіз наукових джерел і нормативних документів, що стосуються цифрової освіти та кібербезпеки;

– порівняльний аналіз програмного забезпечення, яке використовується у професійній підготовці фахівців в сфері цифрових технологій;

– функціональний аналіз, спрямований на виявлення переваг та недоліків для кожного із наведених програмних комплексів з урахуванням вимог освітнього процесу;

– узагальнення та систематизацію отриманих даних для формування висновків щодо їх ефективності впровадження цих програмних рішень у освітній процес.

Таким чином, проведене дослідження дозволяє оцінити роль сучасних програмних інструментів у підготовці фахівців з кіберзахисту та виокремити основні напрями вдосконалення освітнього процесу в сфері цифрових технологій, а саме в практичній підготовці здобувачів.

Актуальністю навчання захисту і основ кібербезпеки є актуальною темою в освіті з кількох ключових причин:

1. Захист даних: поширення інформаційних технологій та загальна цифровізація закладів освіти та освітніх платформ означає, що вони забезпечують обробку і контроль великих об'ємів конфіденційної інформації про здобувачів і викладачів. Забезпечення захисту інформації від витоків та атак зловмисників є одним із найважливіших моментів в організації освітнього процесу.

2. Запобігання перебоям в наданні освітніх послуг: Кібератаки

(наприклад, програми-вимагачі) можуть порушити функціонування освітніх закладів, перериваючи процес, та створюють незручності у освітньому процесі. Ефективне адміністрування допомагає запобігати таким інцидентам.

3. Відповідність законодавству: також є суворі державні вимоги щодо захисту персональних даних здобувачів (наприклад, GDPR в Європі), і освітні установи зобов'язані їх дотримуватися.

4. Підготовка фахівців: Освіта має готувати студентів до реалій сучасного ринку праці, де кібербезпека є невід'ємною частиною будь-якої IT-інфраструктури. Навчальні програми, що включають адміністрування систем кібербезпеки, відповідають попиту на кваліфікованих фахівців.

5. Культура безпеки: Інтеграція теми в освіту має допомогти формуванню загальної культури інформаційної безпеки серед користувачів (здобувачів, викладачів), що повинно знизити ризик впливу шкідливого програмного забезпечення через людський фактор.

Отже, актуальність зумовлена необхідністю захисту інфраструктури, даних та забезпечення безперервності освітнього процесу в цифровому світі.

Виділимо основні навчальні та тренувальні платформи та наведемо їх короткий опис.

Cyber Range (віртуальні полігони):

– Cyberbit Range – симулятор для відпрацювання реагування на кібератаки;

– IBM Security QRadar Cyber Range – кіберполігон з реальними сценаріями та можливостями вирішення загроз;

– EC-Council iLabs – сучасні інтерактивні лабораторні та практичні заняття;

– RangeForce – модульна платформа з практичними тренінгами.

Платформи Capture The Flag (CTF) для спроби пошуку вразливостей:

– Hack The Box;

– TryHackMe;

– CyberSecLabs.

Середовища для проведення віртуальних лабораторій:

– VirtualBox, VMware Workstation – створення навчальних віртуальних машин на, яких можна відпрацьовувати вплив загроз;

– Proxmox VE – інфраструктурне рішення для створення локальних мереж та їх тестування;

– Docker/Kubernetes – для симуляції масованих атак і захисту.

Засоби для аналізу вразливостей і пентестингу:

– Kali Linux – дистрибутив з повним набором інструментів етичного хакінгу;

– Parrot Security OS;

– Nmap / Zenmap – сканування мережевих портів;

– Metasploit Framework – експлуатація вразливостей;

– OpenVAS / Greenbone – комплексне сканування вразливостей;

– Burp Suite – тестування безпеки у середовищі веб;

– Wireshark – аналіз мережевого трафіку.

Системи управління інформаційною безпекою та моніторингу:

– SIEM-системи:

- Splunk;
- IBM QRadar;
- Elastic SIEM.

– IDS/IPS-системи:

- Snort;
- Suricata.

– EDR/XDR-рішення:

- CrowdStrike Falcon;
- Microsoft Defender for Endpoint.

Платформи для моделювання кіберзагроз та атак:

– MITRE ATT&CK Navigator;

– AttackIQ – автоматизоване тестування захищеності;

– Cymulate – моделювання атак та оцінка безпеки;

– CALDERA – інструмент для автоматизації поведінкових сценаріїв атак.

Програмування і моделювання цифрового середовища:

– Cisco Packet Tracer – моделювання мереж;

– GNS3 – емуляція мережевих інфраструктур;

– EVE-NG – розширена платформа для мережевих лабораторій.

Основні та найпоширеніші програмні комплекси для навчання фахівців з кібербезпеки.

Наведемо та проаналізуємо 5 ключових інструментів, які є поширеними засобами в освітній практиці й забезпечують комплексну підготовку фахівців цифрових технологій.

Kali Linux спеціалізований дистрибутив Linux з понад 600 вбудованими інструментами для пентестингу, аналізу вразливостей та мережевої аналітики.

Переваги:

– широкий набір інструментів «все в одному»;

– повністю безкоштовний і відкритий;

– використовується в міжнародних сертифікаціях (CEH, OSCP);

– велика спільнота та навчальні матеріали.

Недоліки:

– високий рівень складності використання;

– високі вимоги до апаратної частини (Технічні характеристики обладнання);

– можливість неправильного використання без належної підготовки.

Metasploit Framework – платформа для тестування безпеки, виявлення вразливостей та моделювання атак.

Переваги:

– підтримує велику базу експлойтів;

– гнучке середовище для автоматизації;

– ідеально підходить для навчання етичному хакінгу;

– інтегрується з Kali Linux.

Недоліки:

– потребує розуміння архітектури атак;

– може бути складним для початкового використання;

– підвищені вимоги до безпечного середовища використання (ізоляція).

Wireshark – це сучасний інструмент для аналізу мережевого трафіку, який широко використовується у практиці SOC-аналітиків і мережевих інженерів.

Переваги:

– безкоштовний і зручний інтерфейс;

– підтримує сотні мережевих протоколів;

– дає реальні навички аналізу трафіку та виявлення атак;

– стандарт у навчанні мережевої безпеки.

Недоліки:

– необхідні глибокі знання мережевих протоколів;

– великий обсяг інформації може ускладнювати аналіз;

– обмежений функціонал для роботи з зашифрованим трафіком.

Hack The Box / TryHackMe (освітні симулятори) – онлайн-платформи, які пропонують сучасні цифрові лабораторії та завдання типу Capture The Flag (CTF) для реального відпрацювання навичок.

Переваги:

– практична підготовка у форматі «навчання через дію»;

– регулярно оновлювані завдання;

– можливість навчатися з будь-якого місця;

– різні рівні складності (від початківців до експертів).

Недоліки:

– обмежений функціонал у безкоштовних версіях;

– потребує стабільного інтернет-з’єднання;

– не всі завдання вказують на теоретичні основи рішень.

Splunk / Elastic SIEM (системи моніторингу безпеки) – аналітичні платформи для збирання, обробки та візуалізації великих обсягів журналів безпеки (SIEM).

Переваги:

– можливість моделювати роботу центру моніторингу безпеки (SOC);

– практичні навички аналізу загроз;

– Elastic SIEM має повністю безкоштовну базову версію;

– потужні функції кореляції подій.

Недоліки:

– Splunk – дуже дорога корпоративна ліцензія;

– високі вимоги до ресурсів системи;

– потребує підготовки з ведення журналів безпеки та побудови правил кореляції.

Висновок. Використання сучасних програмних комплексів у підготовці фахівців з кібербезпеки відіграє ключову роль у формуванні практичних навичок фахівців цифрових технологій, необхідних для роботи в умовах

постійних кіберзагроз. Найпоширеніші інструменти – такі як Kali Linux, Metasploit, Wireshark, Hack The Box та системи SIEM – забезпечують комплексне охоплення сфери пентестингу, аналізу трафіку, моніторингу інцидентів та моделювання реальних атак. Застосування віртуальних середовищ, інструментів аналізу трафіку та засобів моніторингу дає змогу комплексно охопити всі етапи захисту інформаційних систем: від виявлення загроз до реагування на загрози. Подальший розвиток методики має бути спрямований на інтеграцію освітніх платформ з автономними цифровими полігонами, автоматизацію практичних занять та адаптацію завдань під індивідуальний рівень студентів. Разом із перевагами ці платформи мають певні обмеження, що вимагає обережного планування їх інтеграції в освітній процес. Проте їх застосування значно підвищує якість і ефективність підготовки сучасних фахівців цифрових технологій.

Використана література:

1. Андрусенко О. В. Віртуалізація як засіб організації навчального середовища для підготовки ІТ-фахівців. *Інформаційні технології в освіті*. 2020. 12 с.
2. Бондаренко С. В. Методика використання тренажерних систем у підготовці фахівців з кібербезпеки. *Проблеми інформатизації освіти.* 2021. 15 с.
3. Гевко І. В., Сіткар Т. В., Франко Ю. П. Методології аудиту захищеності інформаційно-комунікаційних систем : навчальний посібник для здобувачів ступеня магістр. Тернопіль : Вектор, 2025. 276 с.
4. Гнатюк С. О. Кібербезпека: сучасні загрози та засоби захисту. Київ : [видавництво невідоме], 2019. 240 с.
5. Дьяконов А. В. Аналіз трафіку та моніторинг мережі у навчальному процесі. *Комп'ютерні науки*. 2020. 18 с.
6. Журавльов О. С. Сучасні методи навчання у сфері інформаційної безпеки. Харків : [видавництво невідоме], 2021. 200 с.
7. Франко Ю. П., Солонинка М. В. Особливості формування навичок системного адміністрування серверів у студентів технічних коледжів. *Актуальні проблеми та перспективи технологічної і професійної освіти :* матеріали VII Всеукраїнської науково-практичної інтернет-конференції (Тернопіль, 20–21 квітня 2023 р.). Тернопіль : ТНПУ ім. В. Гнатюка, 2023. С. 87–89.
8. Франко Ю. П., Гевко І. В., Сіткар Т. В., Белюх К. В. Системне адміністрування та безпека інформаційних і комунікаційних систем : лабораторний практикум для студентів другого (магістерського) рівня. Тернопіль : ТНПУ ім. В. Гнатюка, 2023. 138 с.
9. Ящик О., Твердохліб І., Франко Ю., Ожга М. Використання технології блокчейн для забезпечення автоматизації управління освітніми документами. *Наукові записки ТНПУ ім. В. Гнатюка. Сер. Педагогіка*. Тернопіль : ТНПУ ім. В. Гнатюка, 2022. № 2. С. 113–120.
10. HackTheBox Academy [електронний ресурс]. URL : https://academy.hackthebox.com/.
11. Splunk User Guide [електронний ресурс]. URL : https://help.splunk.com/en/splunk-enterprise-security-8/user-guide/8.0.
12. Wireshark Documentation. [електронний ресурс]. URL : https://www.wireshark.org/docs.
13. Kalinin M. Cyber Range Technologies in Cybersecurity Education. *Journal of Cyber Training*. 2021. 14 с.
14. Manson D. Ethical Hacking Foundations. New York : Coursera, 2020. [електронний ресурс]. URL : https://www.coursera.org/learn/packt-ethical-hacking-foundations-cacdd.

References:

1. Andrusenko O. V. (2020). Virtualization as a tool for organizing the learning environment for IT specialists [Virtualizatsiya yak zasib orhanizatsiyi navchalnoho seredovyshcha dlya pidhotovky IT-fakhivtsiv], 12 [in Ukrainian].

2. Bondarenko S. V. (2021). Methodology of using simulator systems in the training of cybersecurity specialists [Metodyka vykorystannya trenazherykh system u pidhotovtsi fakhivtsiv z kiberbezpeky], 15 [in Ukrainian].
3. Hevko I. V., Sitkar, T. V., & Franco Y. P. (2025). Methodologies of auditing the security of information and communication systems: a textbook for master's students [Metodolohiyi audytu zakhyshchenosti informatsiyno-komunikatsiynykh system: navchalnyy posibnyk dlya zdobuvachiv stupenya mahistr…], 276 [in Ukrainian].
4. Hnatyuk S. O. (2019). Cybersecurity: modern threats and protection tools [Kiberbezpeka: suchasni zahrozy ta zasoby zakhystu], 240 [in Ukrainian].
5. Diakonov A. V. (2020). Traffic analysis and network monitoring in the educational process [Analiz trafiku ta monitorynh merezhi u navchalnomu protsesi], 18 [in Ukrainian].
6. Zhuravlov O. S. (2021). Modern teaching methods in the field of information security [Suchasni metody navchannya u sferi informatsiynoyi bezpeky], 200 [in Ukrainian].
7. Franco Y. P., & Solonynka M. V. (2023). Features of forming system administration skills in servers among technical college students [Osoblyvosti formuvannya navychkiv systemnoho administruvannya serveriv u studentiv tekhnichnykh kolledzhiv], 87–89 [in Ukrainian].
8. Franco Y. P., Hevko I. V., Sitkar T. V., & Belyukh K. V. (2023). System administration and security of information and communication systems: laboratory manual for master's students [Systemne administruvannya ta bezpeka informatsiynykh i komunkatsiynykh system: Laboratornyy praktykum dlya studentiv druhoho (mahisterskoho) rivnya], 138 [in Ukrainian].
9. Yashchyk O., Tverdokhlib I., Franco Y., & Ozhga M. (2022). Using blockchain technology to ensure automation of educational document management [Vykorystannya tekhnolohiyi blockchain dlya zabezpechennya avtomatizatsiyi upravlinnya osvitnimy dokumentamy], 113–120 [in Ukrainian].
10. HackTheBox Academy. (n.d.). HackTheBox Academy [Electronic resource]. URL : https://academy.hackthebox.com/
11. Splunk. (n.d.). Splunk User Guide [Electronic resource]. URL : https://help.splunk.com/en/splunk-enterprise-security-8/user-guide/8.0
12. Wireshark Foundation. (n.d.). Wireshark Documentation [Electronic resource]. URL : https://www.wireshark.org/docs
13. Kalinin M. (2021). Cyber range technologies in cybersecurity education. *Journal of Cyber Training*, 14, 1–14.
14. Manson D. (2020). Ethical hacking foundations [Electronic resource]. *Coursera*. URL : https://www.coursera.org/learn/packt-ethical-hacking-foundations-cacdd

N. Shymkiv. The application of specialized data protection software within the educational framework for preparing digital technology specialists.

This article examines and provides practical justification for integrating modern and relevant software tools into the training of cybersecurity professionals within the field of digital technologies particularly in light of the growing scale of cyber threats and the increasing societal impact of digital transformation. The appropriateness of integrating technological tools into the educational process is examined, driven by the need to develop practical skills in incident response, traffic analysis, vulnerability identification, and the simulation of real-world attack scenarios. Traditional teaching methodologies are no longer sufficient, as contemporary cybersecurity practice demands hands-on experience with complex network infrastructures, digital forensics, automated monitoring systems, and penetration testing tools.

The paper analyzes key categories of software employed in cybersecurity education: virtualization environments (such as VirtualBox and VMware Workstation); simulation and gamified training platforms (including TryHackMe and HackTheBox); network traffic analysis tools (notably Wireshark); comprehensive penetration testing frameworks (such as Metasploit Framework); and security information and event management (SIEM) systems like Splunk and the ELK Stack. For each of these tools, the article offers specific recommendations for their integration into laboratory sessions, practical training, and incident simulation exercises.

The pedagogical and methodological advantages of virtual environments are explored, highlighting their capacity to support fully functional simulated laboratories that mirror real-world

networks and systems. Capture-the-Flag (CTF)-style platforms are shown to effectively cultivate skills in ethical hacking and vulnerability assessment often referred to as cyber reconnaissance. Wireshark is identified as a cornerstone tool for teaching network analysis and monitoring, enabling students to inspect traffic patterns and recognize indicators of cyberattacks. Metasploit Framework is presented as one of the most effective instruments for demonstrating end-to-end penetration testing, while SIEM platforms like Splunk and ELK Stack are emphasized as critical for developing the analytical competencies required of cybersecurity specialists.

The article concludes that the comprehensive and strategic use of specialized software significantly enhances the effectiveness of professional training, bridging the gap between academic instruction and real-world cybersecurity practice. It not only strengthens students' ability to counter emerging threats but also fosters a deep, contextual understanding of contemporary attack methodologies and their detection and mitigation. Importantly, the authors propose that future pedagogical development should focus on expanding the use of simulation-based software, integrating automated workflows into practical coursework, and implementing adaptive, individualized learning pathways tailored to students' varying levels of prior knowledge and skill.

Keywords: *Pedagogical methods, educational process, practical training, digital technologies, specialist training, digital transformation, data protection, training system, practical changes.*