КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (2), 2018
ISSN 2663 - 4023

УДК 378.147:004

Бурячок Володимир Леонідович
доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки Київський університет імені Бориса Грінченка, Київ, Україна
OrcID 0000-0002-4055-1494
v.buriachok@kubg.edu.ua

Шевченко Світлана Миколаївна
кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних наук і математики
Київський університет ім. Бориса Грінченка, м. Київ, Україна
OrcID 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Складаний Павло Миколайович
старший викладач кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
OrcID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

ВІРТУАЛЬНА ЛАБОРАТОРІЯ ДЛЯ МОДЕЛЮВАННЯ ПРОЦЕСІВ В ІНФОРМАЦІЙНІЙ ТА КІБЕРБЕЗПЕЦІ ЯК ЗАСІБ ФОРМУВАННЯ ПРАКТИЧНИХ НАВИЧОК СТУДЕНТІВ

Анотація. Кількість хакерських атак та матеріальних збитків, які отримують останнім часом країни світу щороку збільшується. Все це вказує на те, що потреба у фахівцях, здатних виявляти та оцінювати ознаки стороннього кібервпливу, моделювати можливі ситуації такого впливу та прогнозувати їх можливі наслідки, організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної і кібербезпеки та протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ систем і мереж, забезпечити криптозахист власного інформаційного ресурсу тощо, - буде зростати.

В даній статті акцентовано увагу на те, що питання кіберзахисту даних особливо гостро постало в Україні. Адже саме від якості отримуваної інформації й залежить наше майбутнє, зокрема й майбутнє нашої держави. Разом з тим в статті зроблено наголос на те, що жодна педагогічна теорія не буде реалізована в навчальній діяльності, якщо для її впровадження не буде розроблено відповідний алгоритм - алгоритм формування влсне фахових компетенцій майбутніх спеціалістів в області інформаційної та кібербезпеки.

На основі наукової педагогічної літератури в статті визначено поняття «віртуальна лабораторія» та її значення у навчальному процесі закладу вищої освіти. Обґрунтовано актуальність впровадження лабораторії для моделювання процесів в інформаційній та кібербезпеці. Представлено віртуальну лабораторію «навчальний кіберполігон» Київського університету імені Бориса Грінченка та можливості її використання студентами у процесі вивчення технологій в інформаційній та кібернетичній безпеці.

Ключові слова: віртуальна лабораторія; навчальний процес; фахівці в інформаційній та кібербезпеці; практичні навички.

1. ВСТУП

«Хто володіє інформацією, той володіє світом» (Н. Ротшильд). Актуальність даного вислову не втрачається, а, навпаки, набирає нову змістову якість у наш час – глобальної інформатизації. Із збільшенням кількості зростає і роль інформації у розвитку держави, економіки, науки, культури. І тому є очевидним, що захист самої інформації стає пріоритетним, як у всіх сферах суспільства, так і окремої людини.

У річному звіті Cisco за 2017-2018 роки [1] з інформаційної безпеки вказується, що «миттєві атаки» стають усе складнішими, більш частими та тривалими (42% організацій зазнали DDoS-атак цього типу), вірус Nyetya був встановлений на понад 1 млн. комп'ютерів через автоматизовані системи оновлення програм. Більш третини компаній, які були вражені хакерською атакою, понесли матеріальні збитки близько 20% прибутку. За даними спеціалістів «Лабораторії Касперського», протягом року 30,01% комп'ютерів інтернет-користувачів у світі хоча б один раз зазнавали веб-атаки класу Malware [2]. Все це вказує на те, що потреба у фахівцях, які забезпечують захист інформаційних даних, буде зростати. Тому проблема підготовки професіоналів в області кібербезпеки є актуальною.

Щороку українські університети випускають 1,5 тисячі бакалаврів спеціальності «Кібербезпека». Проте, як вказує технічний директор компанії IT Specialist Дмитро Пертащук, ці випускники не мають достатніх практичних навичок, їм потрібно 2-3 роки, щоб зорієнтуватися в галузі та виконувати практичні завдання. Причина такої ситуації полягає в тому, що програми підготовки сьогоднішніх спеціалістів не дають тих навичок, які потрібні на робочому місці [3].

Для розв'язання даної проблеми пропонуються наступні етапи:

1) створення практично орієнтовної програми підготовки фахівців спеціальності 125 Кібербезпека (на практичну та лабораторну складову відводиться 2/3 навчального часу);
2) дуальне навчання, тобто майбутнього фахівця навчають заклади вищої освіти (ЗВО) та роботодавці, при цьому студент поєднує навчання та стажування на реальному підприємстві; залучення фахівців-професіоналів до розробки програм, до проведення практичних та лабораторних занять;
3) сертифікація спеціалістів з інформаційної безпеки згідно міжнародних вимог.

Велику роль у вирішенні зазначеної проблеми відводять формуванню практичних навичок майбутніх фахівців з інформаційної та кібернетичної безпеки. Враховуючи викладене мета даної статті полягає у розкритті можливостей віртуальних лабораторій у навчальному процесі ЗВО та їх використання у підготовці фахівців спеціальності 125 Кібербезпека.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Велика кількість досліджень з проблеми застосування в освітньому середовищі віртуальних лабораторій свідчить про актуальність даного питання [4] – [7].

З'ясуємо сутність поняття «віртуальна лабораторія», визначивши при цьому «віртуальність», «віртуальна реальність» та «навчальна лабораторія».

«Віртуальна реальність – нова технологія безконтактної інформаційної взаємодії, яка створює за допомогою комплексних мультимедіа – операційне середовище, ілюзію безпосереднього входження й присутності в реальному часі». [8, с. 6]. «Навчальна лабораторія — навчально-допоміжна установа, призначена для проведення практичних занять. Оснащена спеціальним обладнанням, апаратурою й матеріалами для проведення

демонстрацій дослідів і виконання самостійних робіт учнів. У вузах створюються при кафедрах і використовуються не лише з навчальною метою, а й для проведення експериментальної науково-дослідної роботи» [9, с. 185]. Поєднуючи ці два поняття, визначаємо «віртуальну лабораторію» (virtual laboratory, V-lab, virtual reality laboratory) як навчальну технологію, яка «дозволяє моделювати поведінку об'єктів реального світу у віртуальному комп'ютерному освітньому середовищі та допомагає тим, хто навчається, оволодівати новими знаннями та вміннями» [10, с. 146-147].

Таку ж думку ми знаходимо у працях Д. Троїцького, який вбачає у віртуальній лабораторії інформаційну систему, яка інтерактивно моделює реальний технічний об'єкт та його суттєві для вивчення властивості із застосуванням засобів комп'ютерної візуалізації [5]. Якщо ставити наголос на навчальну діяльність студентів у таких лабораторіях, то ми згодні з дослідженнями О. Семеніхіної [4], яка зазначає, що віртуальна лабораторія – це віртуальне середовище навчання, яке дозволяє моделювати поведінку об'єктів реального світу в комп'ютерному середовищі і допомагає в оволодінні новими знаннями та вміннями. Така лабораторія може виступати апаратом досліджень різних природних явищ з можливістю побудови їх математичних моделей.

Чинниками створення та впровадження віртуальних лабораторій у навчальний процес ЗВО, з одного боку, став швидкий розвиток інформаційних технологій, а з іншого – велика ціна реального обладнання для проведення лабораторних та практичних занять у різних сферах навчання. Тому, як стверджують більшість науковців, віртуальні технології мають зайняти відповідну нішу у освітній діяльності ЗВО [4] – [7]. Серед переваг застосування віртуальних лабораторій виділяють:

- формування фахових компетенцій, які можуть бути безпосередньо перенесені в реальність;
- підвищення якості самостійної навчально-пізнавальної діяльності;
- зацікавленість у вивченні дисципліни, розвиток мотиваційної діяльності;
- доступність;
- автоматизація операцій;
- постійне удосконалення програмних систем та технологій тощо.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Проведений нами аналіз вимог сучасного роботодавця і системи ІТ компаній дозволив розглянути складові професійної компетентності в структурі особистості інженера, якими має володіти професіонал з інформаційної та кібернетичної безпеки, а саме:

- навички програмування (C/C++, Java, Assembler). Навички написання скриптів;
- поглиблені знання операційних систем;
- розуміння роботи різного зловмисного програмного забезпечення (ПЗ). Досвід аналізу, написання в навчальних цілях такого ПЗ;
- навички реверсивного аналізу програмного забезпечення. Вміння користуватися програмами OllyDbg, IDA. Досвід дослідження функціоналу зловмисного ПЗ;
- загальне розуміння щодо життєвого циклу розробки ПЗ та складних архітектур сервісів та ПЗ, досвіду аналізу ризиків безпеки ПЗ;
- знання веб-технологій: протоколів (HTTP/HTTPS, etc.) та їх структури;
- знання мережевих технологій: TCP/IP стек, DNS, DHCP, SSL/TLS, etc.;
- знання існуючих веб-загроз (XSS, SQL(i), CSRF, (R)LFI, Code injections, Session hijacking, Path traversal, Parameter tampering, etc.) та аудиту ПЗ на них;

- знання у використанні стандартів інформаційної безпеки для ПЗ такі як: OWASP, ENISA, NIST/SANS w/p. Знання наступних стандартів та фреймовркв: ISO270xx CobiT, ITIL; базові знання щодо українського законодавства у сфері ІБ;
- навички планування та звітності щодо складання тест кейсів та їх виконання;
- знання засобів та методів криптографічного захисту(ЦСК, ЕЦП);
- знання методик оцінки ризиків;
- володіння технічною англійською мовою на рівні читання літератури, документації, спілкування в електронному вигляді (пошта, форуми і т.д.);
- знання законодавства в частині інформаційної безпеки.

Вище перераховані компетенції свідчать про те, що проблема формування практичних навичок студентів інформаційної та кібернетичної безпеки є актуальною і потребує вирішення якнайшвидше, - починаючи зі створення сучасного інформаційного середовища для навчання до готовності викладачів впроваджувати та використовувати новітні інформаційні технології у навчальному процесі.

Враховуючи вище згадані чинники, на вимогу сьогодення у цьому навчальному році Київським університетом імені Бориса Грінченка була створена віртуальна лабораторія «Навчальний кіберполігон» (рис. 1).

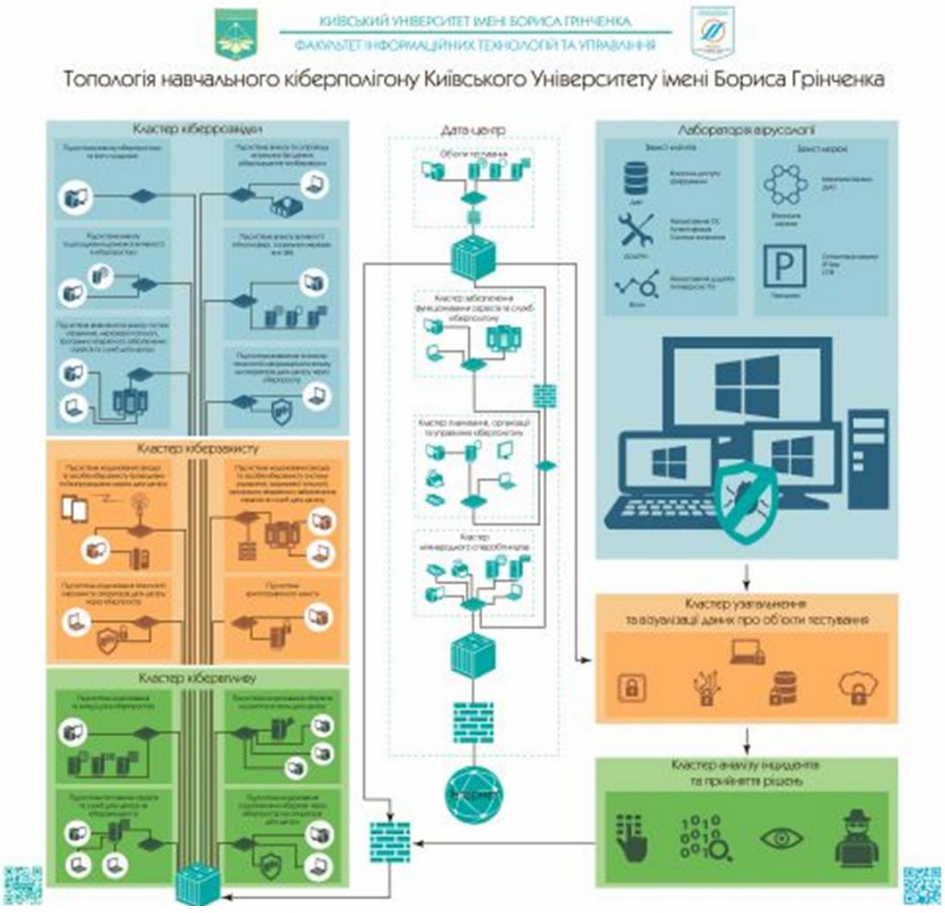

Рис.1. Топологія навчального кіберполігону

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Вище викладені результати нашого дослідження частково окреслили проблему впровадження віртуальних лабораторій у навчальний процес ЗВО, зокрема для

підготовки фахівців з інформаційної та кібернетичної безпеки. На сучасному етапі в Україні дуже гостро постало питання кіберзахисту даних, адже саме від якості отримуваної інформації й залежить наше майбутнє, зокрема й майбутнє нашої держави. Як показує практика навчання в університеті, ніяка педагогічна теорія не буде реалізована в навчальній діяльності, якщо для її впровадження не буде розроблений відповідний алгоритм. Тому надалі вектор наших досліджень буде спрямованим на створення освітньої медіатехнології як цілісної системи навчальної діяльності студентів спеціалізації 125 «Кібербезпека» у процесі вивчення фахових дисциплін.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Cisco Inc. (2018). Звіт Cisco із кібербезпеки за 2018 рік. [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/uk_ua/products/security/security-reports.html [12 нояб. 2018].
[2] Kaspersky Lab. (2018). Kaspersky Security Bulletin 2018. Statistics. [Електронний ресурс]. Режим доступу: https://securelist.ru/kaspersky-security-bulletin-2018-statistics/92906/ [12 нояб. 2018].
[3] Педагогічна преса (2018). Підготовка фахівців із кібербезпеки має бути практично орієнтованою. [Електронний ресурс]. Режим доступу: https://pedpresa.ua/169818-pidgotovka-fahivtsiv-iz-kiberbezpeky-maye-buty-praktychno-oriyentovanoyu.html [12 нояб. 2018].
[4] О. В. Семеніхіна і В. Г. Шамоня, «Віртуальні лабораторії як інструмент навчальної та наукової діяльності», *Педагогічні науки: теорія, історія, інноваційні технології*, №1 (11), сс. 341–345, 2011.
[5] Д. И. Троицкий, «Виртуальные лабораторные работы в инженерном образовании», *Интерактивные электронные технические руководства*, №2, сс. 69–73, 2008.
[6] И. А. Савинов і А. В. Савкина, «Виртуальные лаборатории как средство обучения студентов», *Сборник научных трудов международной научно-практической конференции «Проблемы и достижения в науке и технике»*, №3, Омск, 2016.
[7] Т. В. Никулина і Е. Б. Стариченко, «Виртуальные образовательные лаборатории: принципы и возможности», *Педагогическое образование в России*, №7, 2016.
[8] Я. В. Крупський і В. М. Михалевич, *Тлумачний словник з інформаційно-педагогічних технологій: словник*. Вінниця: ВНТУ, 72 с., 2010.
[9] С. У. Гончаренко, *Український педагогічний словник*. Київ, 375 с., 1997.
[10] О. В. Палагін і М. Г. Петренко, *Тлумачний онтографічний словник з інженерії знань*. Київ: ТОВ «НВП Інтерсервіс», 478 с., 2017.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (2), 2018
ISSN 2663 - 4023

Volodymyr L. Buriachok
Doctor of Technical Sciences, Professor, Head of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
OrcID 0000-0002-4055-1494
v.buriachok@kubg.edu.ua

Svitlana M. Shevchenko
Pnd, Associate Professor of Department of Computer Science and Mathematics
Borys Grinchenko Kyiv University, Kyiv, Ukraine
OrcID 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Pavlo M. Skladannyi
Senior Lecturer of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
OrcID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

VIRTUAL LABORATORY FOR MODELING OF PROCESSES IN INFORMATIONAL AND CYBER SECURITIES AS A FORM OF FORMING PRACTICAL SKILLS OF STUDENTS

Abstract. The number of hacker attacks and material damage that lately has hit the world is increasing every year. All this indicates that the need for specialists capable of detecting and assessing signs of third-party cyber-impacts, modeling the possible situations of such influence and forecasting their possible consequences, organizing and supporting a set of measures to ensure information and cybersecurity and counteract the unauthorized penetration of the opposing sides to their own IT systems and networks, provide cryptosecurity of their own information resource, etc. - will grow. This article focuses on the fact that the issue of cyber-security of data was particularly acute in Ukraine. Indeed, the quality of the information we receive depends on our future, including the future of our state. At the same time, the article stresses that no pedagogical theory will be implemented in educational activities, unless an appropriate algorithm is developed for its implementation - the algorithm of forming the professional competences of future specialists in the field of information and cyber security. On the basis of scientific pedagogical literature, the article defines the concept of "virtual laboratory" and its significance in the educational process of the institution of higher education. The relevance of the implementation of the laboratory for modeling processes in information and cybersecurity is substantiated. The virtual "cyberpolygon training" laboratory of the Borys Grinchenko University of Kyiv and the possibility of its use by students in the process of learning technologies in information and cybernetic security are presented.

Keywords: virtual laboratory; learning process; specialists in information and cybersecurity; practical experience.

REFERENCES

[1] Cisco Inc. (2018). Zvit Cisco iz kiberbezpeky za 2018 rik [Cisco Cybersecurity Report for 2018]. [Online]. Available: https://www.cisco.com/c/uk_ua/products/security/security-reports.html [Nov. 12, 2018]. (In Ukrainian).

[2] Kaspersky Lab. (2018). Kaspersky Security Bulletin 2018. Statistics. [Online]. Available: https://securelist.ru/kaspersky-security-bulletin-2018-statistics/92906/ [Nov. 12, 2018].

[3] Pedagogical Press (2018). Pidhotovka fakhivtsiv iz kiberbezpeky maye buty praktychno oriyentovanoyu [The training of cybersecurity specialists should be practically oriented]. [Online]. Available: https://pedpresa.ua/169818-pidgotovka-fahivtsiv-iz-kiberbezpeky-maye-buty-praktychno-oriyentovanoyu.html [Nov. 12, 2018]. (In Ukrainian).

[4] O. V. Semenikhina and V. H. Shamonya, "Virtual'ni laboratoriyi yak instrument navchal'noyi ta naukovoyi diyal'nosti [Virtual labs as an educational and research tool]," *Pedagogical sciences: theory, history, innovative technologies*, no. 1 (11), pp. 341–345, 2011. (In Ukrainian).

[5] D. Y. Troytskyy, "Virtual'nye laboratornye raboty v inzhenernom obrazovanii [Virtual laboratory works in engineering education]," *Interactive electronic technical manuals*, no. 2, pp. 69–73, 2008. (In Russian).

[6] I. A. Savinov and A. V. Savkina, "Virtual'nye laboratorii kak sredstvo obucheniya studentov [Virtual laboratories as a means of teaching students]," *Collection of scientific papers of the international scientific-practical conference "Problems and achievements in science and technology,"* no. 3, Omsk, 2016. (In Russian).

[7] T. V. Nikulina and E. B. Starichenko, "Virtual'nye obrazovatel'nye laboratorii: printsipy i vozmozhnosti [Virtual educational laboratories: principles and opportunities]," *Pedagogical education in Russia*, no. 7, 2016. (In Russian).

[8] Ya. V. Krups'kyy and V. M. Mykhalevych, *Tlumachnyy slovnyk z informatsiyno-pedahohichnykh tekhnolohiy: slovnyk [Interpretative dictionary of informational and pedagogical technologies: dictionary]*. Vinnitsa: VNTU, 72 p., 2010. (In Ukrainian).

[9] S. U. Honcharenko, *Ukrainian pedagogical dictionary [Ukrayins'kyy pedahohichnyy slovnyk]*. Kyiv, 375 p., 1997. (In Ukrainian).

[10] O. V. Palahin and M. H. Petrenko, *Tlumachnyy ontohrafichnyy slovnyk z inzheneriyi znan' [An ontographic dictionary of expertise on knowledge engineering]*. Kyiv: LLC "NVP Interservis," 478 p., 2017. (In Ukrainian).