УДК 378.147

DOI: 10.30837/nc.2020.3.41

Особливості створення віртуальної лабораторії кібербезпеки для дистанційного навчання

Олександр Лемешко,
доктор технічних наук, професор, завідувач кафедри,

Олександра Єременко,
доктор технічних наук, доцент,

Марина Євдокименко,
кандидат технічних наук,

Євгенія Кузьміних,
кандидат технічних наук,
Харківський національний університет радіоелектроніки

Освіта майбутніх фахівців з кібербезпеки має включати та доповнювати сучасний теоретичний зміст відповідних курсів необхідними практичними навичками [1–4]. У галузі освіти з кібербезпеки передбачається, що викладачі та практичні/лабораторні роботи під їхнім керівництвом повинні мотивувати студентів до виконання та вирішення практичних та проблемно-орієнтованих завдань на реальному обладнанні. Водночас студенти під керівництвом викладача можуть виконувати такі завдання окремо або в групах з обмеженою кількістю учасників навчального процесу, набуваючи таким чином м'яких навичок спілкування та співпраці (soft skills). Така модель є ефективною та забезпечує набуття затребуваних практичних навичок. Крім того, якість освіти та накопичення необхідного рівня знань вимагають, щоб навчальні лабораторії були оснащені необхідним сучасним обладнанням, мережними технологіями, оскільки лише такі умови та робота з реальними технологіями та засобами кібербезпеки дозволять студентам підтверджувати отримані теоретичні знання на практиці.

В останні роки набула популярності та інтенсивного розвитку тенденція віртуалізації як мереж, так і комп'ютерів, що дозволяє розробляти та впроваджувати більш гнучкі типи віртуалізованих лабораторних рішень, у тому числі для дистанційного навчання [1–3, 5–15]. Більше того, функціонал віртуалізації широко підтримується майже всіма постачальниками інформаційних технологій та провайдерів мереж. Збільшується кількість інструментів віртуалізації, а також новітнього мережного обладнання, створених для роботи у віртуальному середовищі (гіпервізори) [1, 5, 8, 9, 12–14]. Отже, саме віртуалізація дозволяє подолати обмеження традиційних мереж та апаратних мережних лабораторій, зважаючи на їхню високу вартість, енергоспоживання, стійкість, обмеженість кількості пристроїв, можливості віддаленого доступу тощо. Все це свідчить про значний

потенціал віртуалізованих лабораторій віддаленого доступу.

У загальному випадку віртуальна лабораторія кібербезпеки для дистанційного навчання використовуватиме відповідне комп'ютерне обладнання (потужні сервери або кластерні сервери). Таким чином, подібні лабораторії дозволяють запустити необхідну кількість пристроїв на одного студента та навіть імітувати складні сценарії роботи в мережі, необхідні для виконання практичних і лабораторних робіт з кібербезпеки (мережної безпеки, тестування на проникнення, цифрової криміналістики тощо). Тому технології віртуалізації наразі вбачаються єдиним способом для розгортання майбутніх лабораторій кібербезпеки для дистанційного навчання та їхньої довготривалої стійкості в умовах карантину та ізоляції.

Віртуалізація дозволяє створювати та використовувати віртуальні середовища для фізичної машини (комп'ютера), мережі чи операційної системи. Крім того, віртуальні середовища дозволяють використовувати різні операційні системи або навіть мережі на одній фізичній машині. Засоби віртуалізації також особливо корисні при викладанні та навчанні в галузі кібербезпеки, оскільки вони ефективно застосовуються для імітації різних видів атак, не завдаючи таким чином шкоди фізичній машині (обладнанню) або цілій мережі користувача [4]. Наприклад, для реалізації деяких атак, таких як «людина посередині» (man-in-the-middle), потрібно щонайменше три комп'ютери для зловмисника та двох жертв, що може бути змодельовано за допомогою трьох віртуальних машин на одній фізичній машині.

Характеристика деяких існуючих віртуальних лабораторій кібербезпеки представлена в таблиці [2, 3, 5–12].

Отже, віртуалізацію можна налаштовувати як на настільному комп'ютері, так і в хмарній інфраструктурі. Віртуальне

Існуючі віртуальні лабораторії кібербезпеки

Назва	Характеристика
ReSeLa [2, 3]	Віртуальна платформа на базі декількох віртуальних машин, яка призначена для надання студентам дистанційного доступу для того, щоб експериментувати зі зловмисним програмним забезпеченням та етичним хакінгом у безпечному середовищі.
DVCL [5]	Розподілена віртуальна комп'ютерна лабораторія для навчання з кібербезпеки та мережних технологій. Лабораторія була реалізована для використання як в умовах дистанційного навчання, так і в умовах кампусу. Це стало можливим завдяки розширенню базової віртуальної лабораторії безпеки (Virtual Security Lab, VCL) розподіленням, центральним керуванням, навчанням з асистуванням і безпекою.
CLaaS (Cybersecurity Lab as a Service) [6]	У CLaaS використано технології хмарних обчислень і віртуалізації з метою проведення віртуальних експериментів з кібербезпеки та отримання практичного досвіду щодо вразливостей, які використовуються для запуску кібератак, методів їх усунення та можливостей посилення захисту кіберресурсів і послуг.
SEED Labs [7]	Надається вбудований образ віртуальної машини, який заздалегідь налаштований на 30 лабораторних робіт з кібербезпеки, які охоплюють широкий спектр тем у галузі комп'ютерної та інформаційної безпеки, включаючи безпеку програмного забезпечення, мережну безпеку, веббезпеку, безпеку операційних систем і безпеку мобільних додатків.
VCCLL (Virtual Cybersecurity Collaborative Learning Laboratory) [8]	Міжінституціональна лабораторія, що пропонує інноваційний, практичний, спільний досвід навчання, спрямований на попередження та зменшення кібератак у режимі реального часу. Використовуючи налагоджений та відносно поширений зловмисний код (експлойти) у віртуальній лабораторії, студенти випробовуватимуть багатовимірні/багатосторонні одночасні атаки та навчатимуться вирішувати, виправляти та протистояти подібним діям у спеціальному спільному середовищі.

VLabNet [9]	Інтегроване середовище для навчання як інформаційній безпеці, так і комп'ютерним наукам з використанням технології віртуалізації на основі програмного забезпечення Xen з відкритим кодом.
Tele-Lab IT-Security [10, 11]	Хмарна платформа для практичної освіти з кібербезпеки.
Розподілена лабораторія ігрового навчання в галузі кібербезпеки та критичних інфраструктур [12]	Розподілена лабораторія для віддаленої лабораторії для навчення кібербезпеки та систем захисту інфраструктури з використанням технологій віртуалізації, хмарних обчислень, а також ігрового навчання (Game-based Learning, GBL).

середовище на робочому столі дозволяє використовувати віртуальні машини з різними операційними системами, які спільно використовують ресурси комп'ютера-хоста [1, 4]. Це дозволяє студентам запускати програми, для яких потрібні різні платформи. Основна проблема віртуалізації на настільному комп'ютері — це достатньо великий розмір віртуальної машини. Крім того, студенти повинні мати високопродуктивні комп'ютери для запуску декількох віртуальних машин. Також слід відмітити, що для віртуальних машин може знадобитися спеціальна конфігурація, наприклад встановлення та налаштування спеціалізованого для кібербезпеки програмного забезпечення та бібліотек, що вимагає додаткових навичок від студентів, яким потрібно виконати конфігурацію самостійно. Альтернативним рішенням у цьому випадку може бути встановлення хмарного середовища для віртуалізації, до якого студенти також можуть отримати віддалений доступ за межами університету.

Основою підготовки курсів для навчання експертів з кібербезпеки наступного покоління є наявність специфічних серверів для швидкого розгортання віртуальної лабораторії кібербезпеки (Cybersecurity Virtual Laboratory, CVLab) та її безпосереднє впровадження у навчальний процес університету.

Відповідно до головної мети CVLab, а саме організації ефективного процесу дистанційного навчання, необхідне виконання низки заходів, а саме:

1. Організація придбання серверного обладнання відповідно до технічних рекомендацій та вимог до обчислювальних ресурсів.

2. Розгортання та запуск CVLab для дистанційного навчання.

3. Тестування CVLab шляхом виконання практичних і лабораторних робіт для перевірки адекватності функціонування середовища, а також усунення можливих помилок.

4. Забезпечення відкритого доступу CVLab для всіх цільових груп, а саме студентів і викладачів університетів України.

5. Організація онлайн-вебінарів і відкритих лекцій щодо можливостей використання CVLab для студентів і викладачів.

6. Поширення інформації про CVLab та її можливості через соціальні мережі та Інтернет-ресурси з метою зацікавлення студентів різних університетів України, де проводиться навчання студентів з кібербезпеки.

7. Ефективний контроль якості віртуального середовища CVLab (внутрішній контроль якості, моніторинг та оцінка).

Зі свого боку, швидке надання віртуальної платформи CVLab для дистанційної освіти буде сприяти забезпеченню повноцінного навчання студентів у період карантину. Така віртуальна платформа буде містити всі необхідні інструменти, програмне забезпечення, а також рекомендації щодо виконання лабораторних і практичних робіт базових навчальних курсів, таких як «Мережна безпека», «Безпека хмарних технологій», «Безпечна розробка програмного забезпечення», «Аналіз шкідливого програмного забезпечення», «Веб-безпека», «Тестування на проникнення», «Етичний хакинг», «Цифрова криміналістика» тощо.

Слід зазначити, що впровадження віртуальної лабораторії кібербезпеки CVLab з метою підвищення ефективності дистанційної освіти відповідає цілям Стратегії кібербезпеки України, а також пріоритетам і напрямам її забезпечення, починаючи від загального підвищення цифрової грамотності громадян до проведення навчань суб'єктів сектору безпеки [16]. Водночас серед переваг впровадження CVLab можна відмітити наступні:

1. *Простота використання та впровадження в навчальний процес*. Після придбання відповідного серверного обладнання та встановлення CVLab студенти можуть виконувати практичні та лабораторні роботи як на сервері, так і на своєму персональному пристрої після завантаження образу віртуальної лабораторії у зручний час. Викладачі можуть створювати вказівки та посібники для лабораторних робіт, тоді як студенти можуть отримувати до них доступ та формувати відгуки.

2. *Універсальність та ефективність*. Завдяки тому, що CVLab буде включати курси навчання, які є частиною базової навчальної програми в галузі кібербезпеки, ця віртуальна платформа зможе охопити більшість університетів, в яких студенти навчаються за цією спеціальністю.

3. *Доступність*. Курси CVLab будуть загальнодоступними. Студенти та викладачі українських університетів зможуть використовувати віртуальну лабораторію для дистанційного навчання в галузі кібербезпеки.

4. *Стійкість*. Використання CVLab є ефективним інструментом для дистанційного навчання не лише під час карантину, але буде корисним у навчальному процесі в будь-який період навчання студентів.

5. *Технічна підтримка*. Передбачається періодичне оновлення платформи та підтримка за потребою.

Література

1. *Segeč P.*, Moravčík M., Kontšek M., Papán J., Uramová J., Yeremenko O. Network virtualization tools-analysis and application in higher education. 17th International Conference on Emerging eLearning Technologies and Applications (ICETA) 2019. Starý Smokovec, Slovakia, 21-22 Nov. 2019 // IEEE, 2019. P. 699-708. DOI: https://doi.org/10.1109/ICETA48886.2019.9040148.

2. *Carlsson A.*, Kuzminykh I., Gustavsson R. Virtual Security Labs Supporting Distance Education in ReSeLa Framework. The Challenges of the Digital Transformation in Education. ICL 2018 // Advances in Intelligent Systems and Computing, Vol. 917. Springer, Cham, 2019. P. 577-587. DOI: https://doi.org/10.1007/978-3-030-11935-5_55.

3. *Carlsson A.*, Gustavsson R., Truksans L., Balodis M. Remote security labs in the cloud ReSeLa. IEEE Global Engineering Education Conference (EDUCON) 2015. Tallinn, Estonia, 18-20 March 2015 // IEEE, 2015. P. 199-206. https://doi.org/10.1109/EDUCON.2015.7095971.

4. *Mouheb D.*, Abbas S., Merabti M. Cybersecurity Curriculum Design: A Survey. Transactions on Edutainment XV // Lecture Notes in Computer Science, Vol. 11345. Springer, Berlin, Heidelberg, 2019. P. 93-107. DOI: https://doi.org/10.1007/978-3-662-59351-6_9.

5. *Haag J.*, Vranken H., van Eekelen M. A Virtual Classroom for Cybersecurity Education. Transactions on Edutainment XV // Lecture Notes in Computer Science, Vol. 11345. Springer, Berlin, Heidelberg, 2019. P. 173-208. DOI: https://doi.org/10.1007/978-3-662-59351-6_13.

6. *Tunc C.*, Hariri S., Montero F.D.L.P., Fargo F., Satam P., Al-Nashif Y. Teaching and Training Cybersecurity as a Cloud Service. 2015 International Conference on Cloud and Autonomic Computing. Boston,

MA, USA, 21-25 Sept. 2015 // IEEE, 2015. P. 302-308. https://doi.org/10.1109/ICCAC.2015.47.

7. *SEED Labs*. URL: http://www.cis.syr.edu/~wedu/seed/lab env.html

8. *Murphy J.*, Sihler E., Ebben M., Lovewell L., Wilson G. Building a Virtual Cybersecurity Collaborative Learning Laboratory (VCCLL) // International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). 2014. P. 1-5.

9. *Powell V.J.*, Davis C.T., Johnson R.S., Wu P.Y., Turchek J.C., Parker I.W. September. VLabNet: the integrated design of hands-on learning in information security and networking // 4th annual conference on Information security curriculum development. 2007. P. 1-7. DOI: https://doi.org/10.1145/1409908.1409918.

10. *Willems C.*, Meinel C. Tele-lab IT-security: An architecture for an online virtual IT security lab // International Journal of Online and Biomedical Engineering (iJOE). 2008. Vol. 4. No. 2. P. 31-37.

11. *Willems C.*, Klingbeil T., Radvilavicius L., Cenys A., Meinel C. A distributed virtual laboratory architecture for cybersecurity training // International Conference for Internet Technology and Secured Transactions. Abu Dhabi, United Arab Emirates, 11-14 Dec. 2011. IEEE, 2011. P. 408-415.

12. *Cano J.*, Hernández R., Ros S., Tobarra L. A distributed laboratory architecture for game based learning in cybersecurity and critical infrastructures // 13th International Conference on Remote Engineering and Virtual Instrumentation (REV). Madrid, Spain, 24-26 Feb. 2016. IEEE, 2016. P. 183-185. DOI: https://doi.org/10.1109/REV.2016.7444461.

13. *Nance K.*, Hay B., Dodge R., Seazzu A., Burd S. Virtual laboratory environments: Methodologies for educating cybersecurity researchers // Methodological Innovations Online. 2009. Vol. 4, No. 3. P. 3-14.

14. *Moritz D.*, Willems C., Goderbauer M., Moeller P., Meinel C. Enhancing a virtual security lab with a private cloud framework // IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE). Bali, Indonesia, 26-29 Aug. 2013. IEEE, 2013. P. 314-320. DOI: https://doi.org/TALE.2013.6654452.

15. *Salah K.*, Hammoud M., Zeadally S. Teaching cybersecurity using the cloud // IEEE Transactions on Learning Technologies. 2015. Vol. 8, No. 4. P. 383-392. DOI: https://doi.org/TLT.2015.2424692.

16. *Стратегія* кібербезпеки України: Указ Президента України від 15.03.2016 р. № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#n11.

03.09.2020