КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№1 (9), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.9.159169
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

Коршун Наталія Володимирівна
доктор технічний наук, доцент, професор кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0003-2908-970X
n.korshun@kubg.edu.ua

Шевченко Світлана Миколаївна
кандидат педагогічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка Київ, Україна
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Складанний 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

ЗАСТОСУВАННЯ СЕРЕДОВИЩА NI MULTISIM ПРИ ФОРМУВАННІ ПРАКТИЧНИХ НАВИЧОК СТУДЕНТІВ СПЕЦІАЛЬНОСТІ 125 «КІБЕРБЕЗПЕКА»

Анотація. Стаття присвячена проблемі формування та розвитку практичних навичок студентів спеціальності 125 «Кібербезпека». Здійснено аналіз фахових компетентностей майбутніх фахівців з кібербезпеки, зокрема, пов'язаних з технічним захистом інформації. Доведено, що використання у навчальному процесі віртуальних лабораторій сприяє підвищенню ефективності освітнього процесу і дозволяє сформувати та удосконалити фахові компетенції майбутнього інженера з кіберзахисту. Освіта стає практично-орієнтованою.
Розглянуто можливості віртуального лабораторного практикуму на базі середовища NI Multisim при вивченні дисциплін «Теорія кіл і сигналів в інформаційному та кіберпросторах», «Компонентна база та елементи схемотехніки в системах захисту інформації», «Сигнали та процеси в системах захисту інформації». Система Multisim використовуються як складова підготовки майбутніх фахівців з кібербезпеки в Київському університеті імені Бориса Грінченка та на практиці довела свою ефективність.

Ключові слова: практичні навички, компетенції інженерно-технічного захисту інформації, віртуальна лабораторія, система Multisim.

1. ВСТУП

Постановка проблеми На сьогоднішній день важливість питання кібербезпеки не викликає сумнівів. Перелік інформаційних продуктів все збільшується, відповідно, зростає ймовірність втілення зловмисних дій з використанням даних, які використовують ці продукти. Вдосконалюються засоби отримання несанкціонованого доступу до інформації і засоби протидії такому доступу. Лише за період з 26 серпня по 01 вересня 2020 року система кіберзахисту

державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала 894 725 підозрілих подій, що на 16% більше, ніж попереднього тижня. Переважна більшість зафіксованих підозрілих подій стосується спроб мережевого сканування (87%) та застосування нестандартних протоколів (11%). Система захищеного доступу державних органів до мережі Інтернет заблокувала 688 686 різних видів атак, що на 45% більше, ніж попереднього тижня. Переважна більшість - це мережеві атаки прикладного рівня (99%) [1].

Забезпечення інформаційної безпеки – процес неперервний і динамічний. Захист інформації є одним з першочергових завдань у сучасному світі. Кіберзахисту підлягають телекомунікаційні системи та мережі, що використовуються суб'єктами господарювання усіх форм власності, органами державної влади, місцевого самоврядування, правоохоронних органів тощо [2].

Разом з тим слід відмітити той факт, що попит на професіоналів в області кібербезпеки продовжує зростати разом з темпами атак і збільшенням бюджету на кібербезпеку. Незбалансованість кількості кваліфікованих фахівців з кібербезпеки поряд з високим попитом на заповнення вакансій з кібербезпеки показали нестачу навичок кібербезпеки [3].

82% роботодавців повідомляють про низький рівень навичок кібербезпеки, 61% компаній вважають, що їх кандидати в області кібербезпеки не відповідають відповідним вимогам [4].

Це також підтверджується у дослідженні [5].

Є очевидним, що формування та розвиток практичних навичок фахівця з кібербезпеки має починатися з перших днів навчання в університеті.

Етапи розв'язання даної проблеми наведені в [6]. Ключовою ланкою є впровадження віртуальних лабораторій, що дозволить освіту майбутніх фахівців зробити практично-орієнтованою.

Аналіз досліджень і публікацій.

Сучасний етап, зокрема це викликано також пандемією Covid-19, характеризується широким використання у професійній освіті інформаційно-моделюючих середовищ навчання. Теоретичні засади моделювання та використання інформаційно-освітнього середовища у закладах вищої освіти досліджували В. Ю. Биков, Л.Л.Макаренко, Л. Ф. Панченко, Li Chao, K.Chilingaryan, M.Despotovic-Zrakic, B.Jovanic, A.Labus, A.Milic, K.Simic та інші науковці. Вони одностайні в тому, що інформаційно-цифрове середовище навчання допомагає вчити та навчатися, що є основою для ефективного розвитку практичних умінь майбутніх фахівців, зокрема кібербезпеки.

Мета роботи. Метою даної статті є опис аспектів проведення лабораторних занять з дисциплін «Теорія кіл і сигналів в інформаційному та кіберпросторах», «Компонентна база та елементи схемотехніки в системах захисту інформації», «Сигнали та процеси в системах захисту інформації» для студентів спеціальності 125 «Кібербезпека» та створення рекомендацій щодо забезпечення ефективного опанування студентами певних практичних навичок.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

У [7] визначено, що ефективним для професійної підготовки фахівців є поєднання діяльнісного й компетентнісного підходів, перший з яких передбачає застосування активних методів навчання, які дозволяють студентам використовувати засвоєні знання

в практично-орієнтованій діяльності, а другий - використання спеціальної методології з урахуванням галузевої специфіки підготовки кадрів. Тут же зазначається, що основою теоретичної бази побудови систем забезпечення кібербезпеки є використання математичних моделей, зокрема цифрового імітування, моделювання систем.

Існує величезний спектр технічних засобів, що дозволяють отримати несанкціонований доступ до інформації з метою досягнення найрізноманітніших цілей: від особистої помсти до промислового шпіонажу. Згадаємо тільки деякі засоби отримання конфіденційної інформації за допомогою технічних засобів. Це і величезне розмаїття так званих закладних пристроїв, що таємно встановлюються в місцях можливого знаходження об'єктів спостереження або підключаються до каналів зв'язку, які використовуються об'єктами. Це і системи прослуховування, що дозволяють одночасно контролювати декілька приміщень, і спрямовані мікрофони різноманітних модифікацій, пристрої звукозапису тощо. Окремої уваги заслуговують засоби перехоплення інформації в різноманітних каналах зв'язку (дротових, бездротових), лазерні системи акустичної розвідки, засоби для проведення прихованої фотозйомки. Це тільки малий перелік того, що є на сьогодні на озброєнні потенційних зловмисників.

Фахівець в галузі інформаційної та кібернетичної безпеки повинен орієнтуватися в таких засобах, мати глибоке розуміння фізичних явищ, на яких базується побудова і робота таких засобів та, відповідно, адекватно використовувати засоби протидії, комбінувати їх та вдосконалювати чи навіть створювати нові. Необхідними є знання теорії передавання сигналів, розуміння роботи систем зв'язку і передачі інформації, оскільки без цього неможливий аналіз технічних каналів можливого витоку інформації. Важливим є здобуття навичок вимірювання електричних величин, обробки експериментальних даних, практичне вивчення принципів побудови і функціонування логічних елементів, пристроїв комбінаційного і послідовних типів та інтегральних мікросхем, побудова та аналіз діаграм електричних величин та характеристик пристроїв. Такі навички можна віднести до «професійних компетентностей ..., що закладають основу наступних класів компетентностей» [8].

Таким чином, необхідно сформувати у студентів базу фундаментальних знань, що складають основу інженерно-технічного захисту інформації, і без яких буде неможливим розв'язання ними завдань такого характеру в процесі їх діяльності як фахівців. На створення такої бази спрямоване вивчення ряду дисциплін, що забезпечують формування спеціальних компетентностей.

Дисципліни «Теорія кіл і сигналів в інформаційному та кіберпросторах», «Компонентна база та елементи схемотехніки в системах захисту інформації», «Сигнали та процеси в системах захисту інформації», які мають на меті забезпечення ряду фахових компетентностей спеціальності 125 «Кібербезпека», серед яких:

- здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;
- здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження;
- здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) [9].

Сучасний випускник спеціальності 125 «Кібербезпека» повинен вміти застосовувати в професійній діяльності знання, навички та практики щодо структур

сучасних обчислювальних систем, методів і засобів обробки інформації; забезпечувати процеси захисту інформаційно-телекомунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; проектувати та реалізовувати комплексні системи захисту інформації відповідно до вимог нормативних документів; визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в інформаційно-телекомунікаційних системах; використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах [9].

У [6] приводиться визначення віртуальної лабораторії як навчальної технології, яка «дозволяє моделювати поведінку об'єктів реального світу у віртуальному комп'ютерному освітньому середовищі та допомагає тим, хто навчається, оволодівати новими знаннями та вміннями». Така лабораторія може виступати апаратом досліджень різних явищ з можливістю побудови їх математичних моделей. Зважаючи на високу вартість реального обладнання, необхідного для проведення занять для здобуття практичних навичок, та його достатньо об'ємний перелік, впровадження віртуальних технологій для вивчення фізичних процесів у системах захисту інформації, компонентної бази таких систем та їх моделювання є актуальним завданням. Під час лабораторних занять студент проводить певні досліди, набуває практичних навичок роботи з лабораторним обладнанням, а також вивчає методику проведення експериментальних досліджень. В умовах, коли технології дистанційного навчання отримують все вагомішу роль в організації освітнього процесу, проведення лабораторних занять у віртуальних середовищах постає на часі. Не є винятком і набуття навичок в рамках вивчення дисциплін, наведених вище.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Вивчення дисципліни «Компонентна база та елементи схемотехніки в системах захисту інформації» має на меті надання студентам знань та навичок щодо принципів побудови електронних схем цифрових елементів і функціональних вузлів, схемотехніки аналогових і цифрових пристроїв, що забезпечують аналогову і цифрову обробку сигналів в електронних обчислювальних машинах, принципів функціонування комп'ютерної техніки та оброблення цифрової інформації, а також вміння використовувати отримані знання при роботі з обладнанням в сфері інформаційних технологій.

При вивченні даних питань широко використовується імітаційне моделювання електронних пристроїв. Лабораторні роботи на основі комп'ютерної техніки дозволяють моделювати складні об'єкти, процеси та явища, досліджувати закономірності роботи пристроїв чи вузлів навіть за відсутності відповідного лабораторного устаткування.

Існує досить великий перелік середовищ, призначених для розробки різноманітних електронних пристроїв та емуляції електричних схем. Серед них можна назвати OrCAD, Electronics Workbench, Proteus Design, Micro-Cap, NI Multisim та інші. В роботі [10] проведено класифікацію та порівняння ряду систем автоматизованого проектування, які можливо застосовувати для вивчення та проектування електронних пристроїв, радіоелектронних засобів, інтегральних схем, друкованих плат тощо.

ISSN 2663 - 4023

На нашу думку, найбільш доцільним для формування професійних навичок під час електротехнічної підготовки майбутніх фахівців з кібербезпеки є система Multisim, яка ілюструє віртуальну електричну лабораторію на персональному комп'ютері. Моделювання та аналіз віртуальних електричних схем засновані на особливостях програми Multisim. Вона містить у своєму складі практично всі відомі елементи сучасних електричних кіл: джерела постійної і змінної напруги та струму; активні, індуктивні й ємнісні елементи; трансформатори, електричні машини, а також інформаційно-вимірювальне обладнання: амперметри і вольтметри змінного й постійного струму, ватметри, мультиметри, осцилографи тощо. При цьому параметри будь-яких елементів можна змінювати для отримання реальних процесів.

Аналіз деяких програмних продуктів, використання яких можливе при організації навчального процесу, виконано в роботі [12], де автор для вирішення завдання навчання студентів також обґрунтовано обрав середовище NI Multisim 10 Analog Devices Edition. Саме середовище Multisim компанії National Instruments отримало досить широке розповсюдження в навчальних закладах. Це програмне забезпечення для інтерактивного SPICE-моделювання та аналізу електричних кіл, що використовуються в схемотехніці, проектуванні друкованих плат і комплексному тестуванні. Платформа дозволяє об’єднати процеси розробки електронних пристроїв і тестування на основі технології віртуальних приладів. Бібліотека NI Multisim містить величезну кількість електронних компонентів. Крім того, можна використовувати велику кількість моделей аналогових та цифрових пристроїв, засобів аналізу. Наявність контрольно-вимірювальних приладів, що за характеристиками та зовнішнім виглядом близькі до промислових аналогів, робить середовище особливо зручним. Моделювання електричних схем пристроїв та візуалізація результатів сприяє кращому розумінню функціонування схем реальних. Електронна система моделювання Multisim імітує реальне робоче місце дослідника - лабораторію, обладнану вимірювальними приладами, що діють в реальному масштабі часу. З її допомогою можна створювати, моделювати та досліджувати як прості, так і складні пристрої.

Робота з електронною системою моделювання Multisim включає в себе три основних етапи: створення схеми, вибір і підключення вимірювальних приладів та активацію схеми – розрахунок процесів, які відбуваються в пристрої, що досліджується.

Multisim має кілька розділів бібліотеки компонентів (рис.1), які можуть бути використані при моделюванні. Це джерела сигналів, пасивні елементи, напівпровідникові елементи, аналогові мікросхеми, логічні цифрові мікросхеми, індикаторні пристрої, контрольно-вимірювальні прилади.

ISSN 2663 - 4023

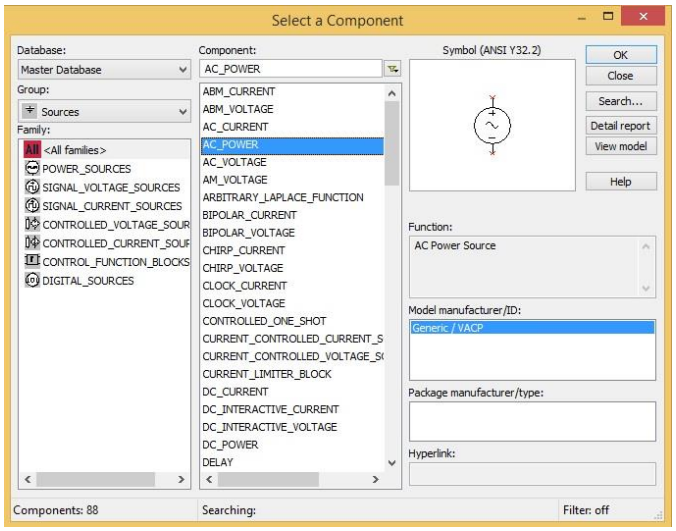


Рис.1. Бібліотека компонентів - Source Components

Контрольно-вимірювальні прилади мають повноцінний набір функцій та можливості налаштування відповідно до задач користувача. До прикладу, для осцилографа (рис.2) можливе роздільне регулювання чутливості, регулювання зміщення по вертикалі, вибір режиму по входу, режимів розгортки, прокрутка зображення по горизонталі і його сканування, інвертування зображення тощо.

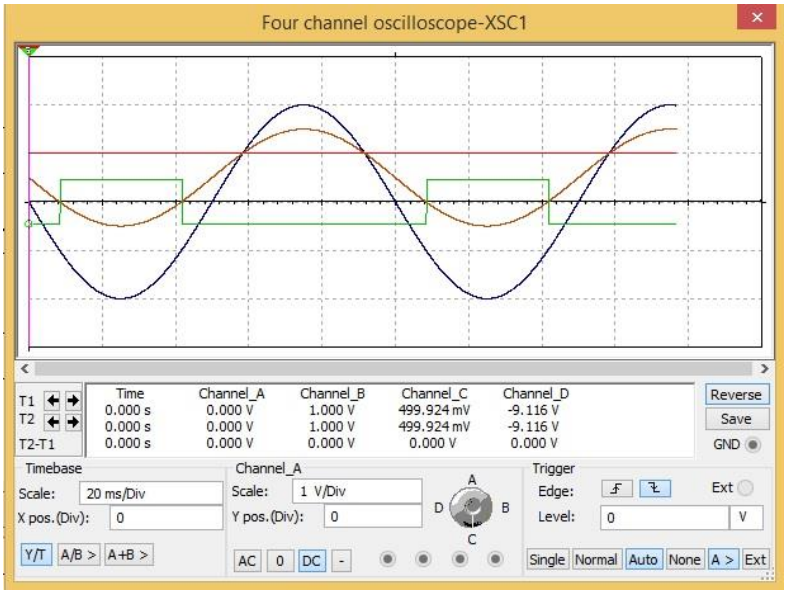
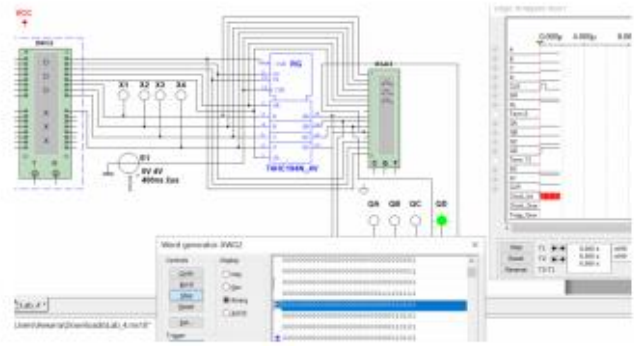


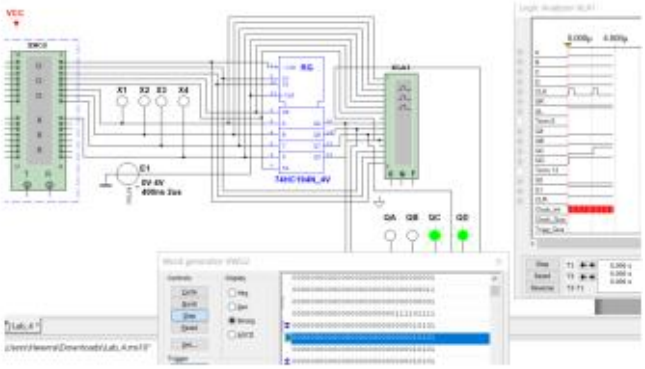
Рис.2. Осцилограф

ISSN 2663 - 4023

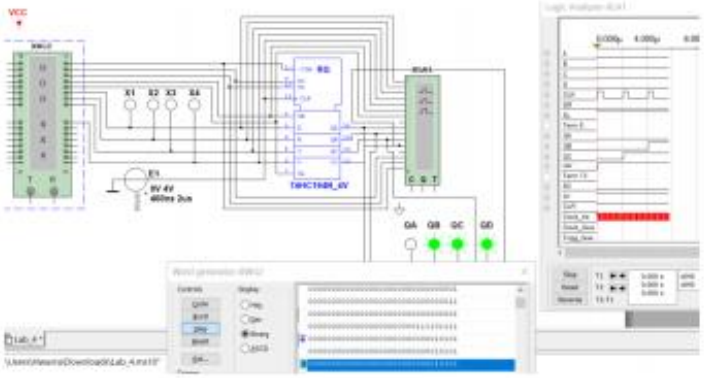
Крок 1



Крок 2



Крок 3



Крок 4

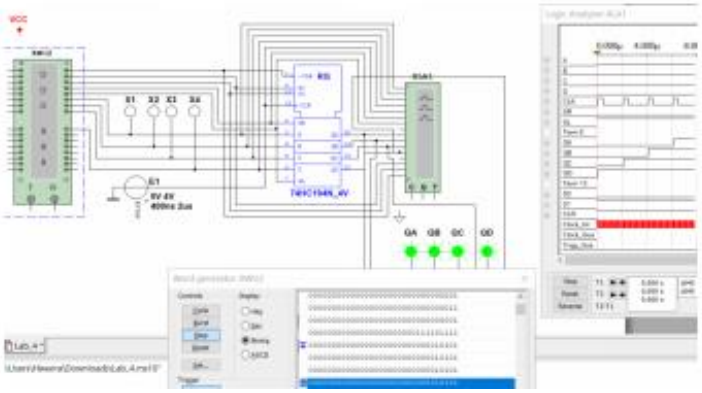


Рис.3. Дослідження регістру в NI Multisim

Віртуальна лабораторія, яку створює середовище Multisim, дозволяє здійснювати розрахунок і аналіз процесів, що мають місце в радіоелектронному пристрої. Приклад дослідження регістру в рамках лабораторної роботи зображено на рис.3. Порядок роботи з віртуальними приладами повністю віддзеркалює роботу у лабораторії реальній. В процесі моделювання можна змінювати параметри елементів, видаляти або додавати радіоелементи, підключати прилади до інших контрольних точках схеми тощо. Наявна можливість додатково провести інші види аналізу: спектральний аналіз, розрахунок чутливості і розкиду характеристик схеми при зміні параметрів компонентів, аналіз спектра внутрішніх шумів, розрахунок нелінійних спотворень, аналіз впливу варіацій параметра будь-якого елементу схеми, аналіз впливу зміни температури на характеристики пристрою, розрахунок передавальної функції, розрахунок чутливості і розкиду характеристик схеми при зміні параметрів компонентів.

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

На базі середовища NI Multisim було проведено ряд лабораторних робіт з вивчення компонентної бази систем захисту інформації. Широкі можливості середовища дозволяють досягти формування ряду базових компетентностей, що стануть підґрунтям для подальшого формування фахових компетентностей випускника спеціальності 125 «Кібербезпека», зокрема, при вивченні дисциплін «Фізичні основи захисту інформації», «Захист інформації в інформаційно-комунікаційних системах», «Теоретичні аспекти захищених інформаційно-комунікаційних технологій», «Системи технічного захисту інформації» та проходженні виробничої практики.

Навчально-інформаційні середовища, що функціонують на базі технології мультимедіа та системи віртуальної реальності, доводять високі дидактичні можливості та педагогічну доцільність їх застосування, забезпечують інтеграцію практичних умінь з теоретичними знаннями. Дозволяють стверджувати необхідність і пріоритетність їх розробки та впровадження в процес підготовки студентів в закладах вищої школи.

Напрямок подальших досліджень спрямований на теоретичне обґрунтування, розробку та впровадження інформаційно-моделюючого середовища у процесі вивчення дисципліни «Теорія ризиків».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Оперативна інформація Держспецзв'язку щодо захисту державних інформаційних ресурсів за період з 26 серпня по 01 вересня 2020 року. [Електронний ресурс]. Режим доступу: https://www.cip.gov.ua/ua/news/operativna-informaciya-derzhspeczv-yazku-shodo-zakhistu-derzhavnikh-informaciinikh-resursiv-za-period-z-26-serpnya-po-01-veresnya-2020-roku [02.09.2020].

[2] Ю. Сачук, «Нормативно-правові засади забезпечення професійної підготовки фахівців із кібербезпеки та захисту інформації», *Молодь і ринок*. №12 (167). С. 45-50, 2018.

[3] 110 Must-Know Cybersecurity Statistics for 2020. [Електронний ресурс]. Режим доступу: https://www.varonis.com/blog/cybersecurity-statistics/ [02.09.2020].

[4] 2017 ISSA ESG Survey Results [Електронний ресурс]. Режим доступу: https://www.members.issa.org/page/2017_issaesg_surv [02.09.2020].

[5] Педагогічна преса (2018). Підготовка фахівців із кібербезпеки має бути практично орієнтованою. [Електронний ресурс]. Режим доступу: https://pedpresa.ua/169818-pidgotovka-fahivtsiv-izkiberbezpeky-maye-buty-praktychno-oriyentovanoyu.html [09.06.2020].

[6] В.Л. Бурячок, С.М. Шевченко, П.М. Складаний, «Віртуальна лабораторія для моделювання процесів в інформаційній та кібербезпеці як засіб формування практичних навичок студентів», *Кібербезпека: освіта, наука, техніка*. № 2(2). С. 98-104, 2018.

[7] С. Мельник, «Концептуальні основи організації професійної підготовки майбутніх фахівців із кібербезпеки», *Педагогічні науки: теорія, історія, інноваційні технології*. № 10 (64). С. 79-88, 2016.

[8] В. Бурячок, В. Богуш, «Рекомендації щодо розробки та реалізації моделі професійних компетентностей у сфері підготовки фахівців для національної системи кібербезпеки», *Захист інформації.* №2 (20). С. 72-78, 2018.

[9] Освітньо-професійна програма. 125.00.01. Безпека інформаційних і комунікаційних систем першого (бакалаврського) рівня освіти. Київський університет імені Б. Грінченка, 2018. [Онлайн] Режим доступу: http://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitu/2018/2019_bak_op_kiber.pdf [09.06.2020]

[10] І.А. Твердохліб, «Навчання фізико-технічних дисциплін майбутніх вчителів інформатики з використанням комп'ютерного моделювання», Науковий часопис НПУ імені М. П. Драгоманова. Серія 2 : Комп'ютерно-орієнтовані системи навчання. - 2015. - № 17. - С. 127-132. - Режим доступу: http://nbuv.gov.ua/UJRN/Nchnpu_2_2015_17_24 [09.06.2020]

[11] Хернитер М.Е. Электронное моделирование в Multisim / М.Е. Хернитер. – М.: ДМК, 2010. – 488 с.

[12] В.В. Макаренко, «Использование NI Multisim для пояснения процессов демодуляции АМ-сигналов», *Фізико-математична освіта (ФМО)*. № 1(19). С. 122-129, 2019.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (9), 2020
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

Nataliia V. Korshun
Doctor of Technical Sciences, associate professor, Professor of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-4055-1494
n.korshun@kubg.edu.ua

Svitlana M. Shevchenko
PhD, Associate Professor of Department of Information and Cyber Security
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

APPLICATION OF NI MULTISIM ENVIRONMENT IN THE PRACTICAL SKILLS BUILDING FOR STUDENTS OF 125 "CYBERSECURITY" SPECIALTY

Abstract. The article is devoted to the problem of practical skills building and development of students majoring in 125 "Cybersecurity". An analysis of the professional competencies of future cybersecurity professionals, in particular, related to technical protection of information. It is proved that the use of virtual laboratories in the educational process helps to increase the efficiency of the educational process and allows to form and improve the professional competencies of the future cybersecurity engineer. Education becomes practice-oriented. The possibilities of a virtual laboratory workshop based on the NI Multisim environment are considered in the study of disciplines "Theory of circles and signals in information and cyberspace", "Component base and elements of circuitry in information security systems", "Signals and processes in information security systems". The Multisim system is used as part of the training of future cybersecurity professionals at Borys Grinchenko Kyiv University and has proven its effectiveness in practice.

Keywords: practical skills, competences of engineering and technical protection of information, virtual laboratory, Multisim system.

REFERENCES

[1] Operational information of the State Special Communications Service on the protection of state information resources for the period from August 26 to September 1, 2020. [Electronic resource]. Available: https://www.cip.gov.ua/ua/news/operativna-informaciya-derzhspeczv-yazku-shodo-zakhistu-derzhavnikh-informaciinikh-resursiv-za-period-z-26-serpnya-po-01-veresnya-2020-roku [02.09.2020].

[2] Yu. Sachuk, "Regulatory framework for providing training for cybersecurity and information security professionals", *Youth and the market*. №12 (167). Pp. 45-50, 2018.

[3] 110 Must-Know Cybersecurity Statistics for 2020. [Electronic resource]. Available: https://www.varonis.com/blog/cybersecurity-statistics/ [02.09.2020].

[4] 2017 ISSA ESG Survey Results [Electronic resource]. Available: https://www.members.issa.org/page/2017_issaesg_surv [02.09.2020].

[5] *Pedagogical Press* (2018). The training of cybersecurity professionals should be practice-oriented. [Electronic resource]. Available: https://pedpresa.ua/169818-pidgotovka-fahivtsiv-izkiberbezpeky-maye-buty-praktychno-oriyentovanoyu.html [09.06.2020].

[6] V. L. Buryachok and S.M. Shevchenko and P.M. Skladannyi, "Virtual laboratory for modeling processes in information and cybersecurity as a means of forming practical skills of students", *Cybersecurity: education, science, technology*. № 2 (2). Pp. 98-104, 2018.

[7] S. Melnyk, "Conceptual foundations of the organization of professional training of future specialists in cybersecurity", *Pedagogical sciences: theory, history, innovative technologies.* № 10 (64). Pp. 79-88, 2016.

[8] V. Buryachok and V. Bogush, "Recommendations for the development and implementation of a model of professional competencies in the field of training for the national cybersecurity system", *Information security*. №2 (20). Pp. 72-78, 2018.

[9] Educational and professional program. 125.00.01. Security of information and communication systems for first (bachelor's) level of education. Borys Grinchenko Kyiv University. 2018. [Online]. Available: http://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitu/2018/2019_bak_op_kiber.pdf [09.06.2020].

[10] I.A. Tverdokhlib, "Teaching physical and technical disciplines of future teachers of computer science using computer modeling", *Scientific Journal of NPU named after MP Drahomanov. Series 2: Computer-based learning systems.* - 2015. - № 17. - P. 127-132. Available: http://nbuv.gov.ua/UJRN/Nchnpu_2_2015_17_24 [09.06.2020].

[11] Herniter M.E. Electronic modeling in Multisim / ME Herner. - M .: DVK, 2010. - 488 p.

[12] V.V. Makarenko, "Using NI Multisim to explain the processes of demodulation of AM signals", *Physical and Mathematical Education (FMO).* № 1 (19). Pp. 122-129, 2019. p.