ВИСТУПИ РЕГІОНАЛЬНОЇ КОНФЕРЕНЦІЇ МСЕ ДЛЯ КРАЇН ЄВРОПИ ТА СНГ «ЦИФРОВЕ МАЙБУТНЄ НА ОСНОВІ 4G/5G»

Хмелевський Ростислав Миколайович, старший викладач
Державний університет
телекомунікацій
м. Київ

ШЛЯХИ ВДОСКОНАЛЕННЯ ПРОФЕСІЙНОЇ ПІДГОТОВКИ КВАЛІФІКОВАНИХ ФАХІВЦІВ В ОБЛАСТІ КІБЕРБЕЗПЕКИ

Пропонується підхід до адаптації змісту підготовки фахівців в системі вищої освіти України для сучасних і перспективних потреб для кібербезпеки за фахом «кібернетична безпека» виходячи з критеріїв щодо професійних компетентностей фахівця з кібербезпеки.

В умовах загальносвітових тенденцій становлення глобального інформаційного простору і формування інформаційного суспільства в Україні, все більше зростає залежність стану інформаційної безпеки (ІБ) від сучасних кіберзагроз ІБ, прояв яких може завдати непоправної шкоди усій системі держави. Національна безпека держави залежить від забезпечення ІБ, впливає на національні інтереси країни в інформаційній сфері. В цілях ефективного відображення загроз кібербезпеки, однією зважливих вимог часу стають питання вдосконалення професійної підготовки фахівців в області кібербезпеки.

Указ Президента України «Про Стратегію національної безпеки України» визначив одні з пріоритетних напрямів національної безпеки, зокрема, забезпечення захищеності державних інформаційних ресурсів від кібератак, вдосконалення професійної підготовки в області ІБ, впровадження загальнонаціональних освітніх програм із залученням навчальних закладів до розробки і реалізації заходів з кібербезпеки та кіберзахисту [1].

На безпеку роботи ключових державних інформаційних систем здійснюють вплив сучасні загрози. В 2017 році ІТ-інфраструктури світових компаній піддалися кібератакам шифрувальників: WannaCry, XDATA. А 27 червня з'явилась нова версія вимагача Petya.A. Від атаки постраждало більше 80 українських компаній в усіх галузях економіки. Вектор «шифрувальника» стандартний: таргетований користувач отримує лист з вкладенням або посиланням на шкідливий файл. Після відкриття файлу відбувається експлуатація уразливості CVE-2017-0199, далі завантажується файл hxxp://84.200.16.242/myguy.xls.

За даними центру кібербезпеки США одними з ключових ризиків 2017 року можуть стати: *захист периметру безпеки*, *ідентифікація та автентифікація*, *управління ресурсами* (навчання фахівців з достатньою кваліфікацією для роботи з критичними системами), управління обліковими записами, тощо.

Президент Київського відділення ISACA О. Янковський вказує на те, що в Україні є фундаментальна проблема з точки зору кібербезпеки – у нас не застосовуються світові стандарти з кібербезпеки і в країні не проводиться робота з підготовки організацій до кібератак. Необхідний перехід до міжнародних кращих практик – ISO-27000 та NIST.

Так само було відзначено, що вузи повинні готувати студентів за міжнародними стандартами. В Україні повинні бути визнані на державному рівні міжнародні сертифікації по Forensic, кібербезпеці, ІТ-аудиту, ІТ-управлінню [2].

Для вдосконалення професійної підготовки в області кібербезпеки в навчальних закладах потрібно рішення цілого комплексу важливих і невідкладних завдань.

Формування спеціальних професійних якостей, необхідних для реалізації професійних компетенцій майбутніх фахівців кібербезпеки, здійснюється в процесі професійної підготовки – вивчення спеціальних навчальних дисциплін з освітньої та навчальної складовими відповідно до профілей освітньо-наукових програм і відповідних стандартів вищої освіти нового покоління і мають формуватися на основі компетентнісного підходу [3].

Виходячи зі світових освітніх тенденцій в підготовці нового покоління фахівців кібербезпеки, пропонується і далі удосконалювати їх підготовку, наприклад для дисципліни кафедри ІКБ «Захист інформації в інформаційно-комунікаційних системах і мережах» за чотирма передбаченими підсистемами безпеки у таких напрямках:

1. Гармонізація національних стандартів з їх міжнародними аналогами з кібербезпеки (ISO/IEC 2700X, ITU X.805, CMU/SEI 2004-TR-015, NIST SP 800-61).
2. Основи організації процесів розслідування інцидентів Digital forensic.
3. Ознайомлення з основами Websecurity, архітектурою побудови Web-ресурсів, основними уразливостями Web-ресурсів (SQL-ін'єкція, XSS, bruteforce).
4. Побудова СЗІ КС на сучасних платформах сертифікованого ПЗ.
5. Ознайомлення з міжнародним досвідом програми ENGENSEC по методам дослідження загроз Malware analysis і застосування засобів антивірусного захисту.
6. Виконувати аудит аналізу ризиків щодо можливості здійснення кіберзагроз на предмет виявлення та локалізації вузьких місць в СЗІ. Розробляти рекомендації щодо підвищення ефективності існуючих механізмів безпеки КС.
7. Виконувати перевірку сайтів на наявність комп'ютерних вірусів. Перевірка сайтів на наявність вірусів VirusTotal, Google, McAfee, Symantec та Trend Micro.
8. Ознайомлення з основними засобами віртуалізації мереж з кібербезпеки. Відпрацювання технологій виявлення кібератак і протидії їм, ліквідація наслідків застосування і відновлення нормальних режимів функціонування мереж управління кіберінфраструктури.
9. Межмережеве екранування (Brandmauer ICS/SCADA).
10. Забезпечення безпеки в КС на базі програмно-апаратного забезпечення Cisco Packet Tracer та IBM (AppScan, Network and Endpoint Protection).

Рішення комплексу завдань на державному рівні по ІБ [3] і підготовка фахівців зі спеціальних дисциплін, на думку автора роботи, може допомогти адаптувати зміст підготовки фахівців у ВНЗ для сучасних і перспективних потреб інформаційної та кібербезпеки.

Список використаних джерел:

1. «Про Стратегію кібербезпеки України». Указ Президента України № 96/2016 від 27 січня 2016 року. – [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/287/2015

2. Проблеми в сфері кібербезпеки в Україні. – [Електронний ресурс]. – Режим доступу: https://www.pravda.com.ua/columns/2017/02/15/7135442/

3. В.Л. Бурячок, І.Р. Пархоме, М.М. Степанов, В.Б. Толубко. «Питання та актуальні завдання підготовки фахівців з кібернетичної безпеки галузі знань» інформаційні технології ««, Сучасний захист інформації, № 2, С. 4-9, 2016.

4. Хмелевський Р.М. Тези. «Інформаційна безпека як одна з основ забезпечення ефективності роботи державного управління». Матеріали міжнародної науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології» Том IV «Сучасні технології інформаційної безпеки» Київ, ДРП. 17-20 листопада 2015 – С.155-158.

Viktor Vyshnivskyi, Volodymyr Sokolov
State University of Telecommunication
Kyiv, Ukraine

LABORATORY COMPLEX “CYBER RANGE”

These theses contain information about the laboratory “Cyber Range” of the Department of Information and Cyber Security.

State University of Telecommunications in cooperation with the European Union participated in the Tempus project #544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR “Educating the Next