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

Generation Experts in Cyber Security: the New EU-recognized Master's program" (ENGENSEC) [1].

As a result, it was created a unique complex "Cyber Range", which is used during the sessions in bachelor and master degrees:

1. Security Software Development.
2. Advanced Networks and Cloud Security.
3. Malware.
4. Penetration Testing and Ethical Hacking.
5. Wireless and Mobile Security.
6. Web-security.

Cyber range is a virtual environment where computer networks, attackers, and victims are modeled. Hardware supports virtualization at the processor level, and allows you to use *docker* virtualization environment on it (fig. 1).

The *OpenStack* platform is deployed with ready-made network solutions based on *docker*.

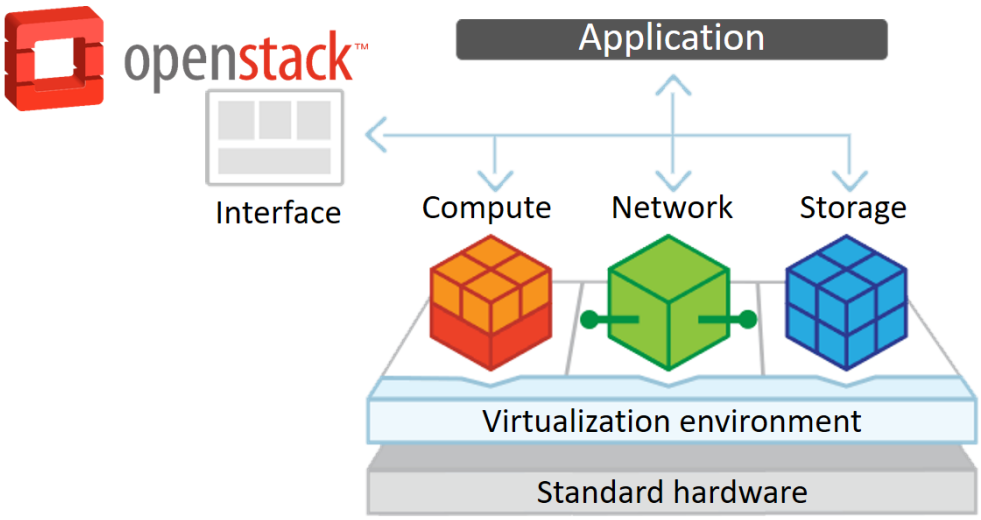

Fig. 1. Block scheme of the OpenStack platform work

Physically, this virtual environment is a switch, a controller and two compute nodes. Network equipment Mikrotik is used as a switch to create a virtual network and exchange control and data information (fig. 2).

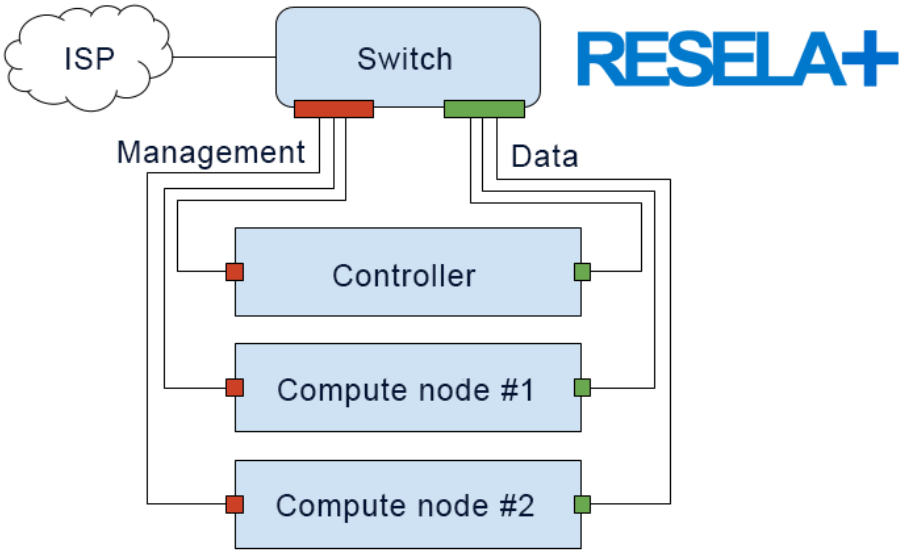

Fig. 2. Structural elements of the cyber range

Access to virtual laboratory and practical work provides by the web-interface RESELA+, developed by Blekinge Institute of Technology (Sweden).

Within the framework of participation in the European Tempus Project, the staff of the State University of Telecommunications developed a course on "Wireless and Mobile Security", which was implemented by all project participants. The laboratory workshop was published in both English [2] and Ukrainian [3].

The work of cyber range is provided by 3 Dell servers, 15 workstations, and router Mikrotik (see fig. 3) received within the project by the European Commission.

Fig. 3. Process of the cyber range hardware installation

We are using a library with more than 300 tools to provide laboratory works and workshops:

1. Information Gathering.
2. Vulnerability Analysis.
3. Wireless Attacks.
4. Web Applications.
5. Exploitation Tools.
6. Stress Testing.
7. Forensics Tools.
8. Sniffing and Spoofing.
9. Password Attacks.
10. Maintaining Access.
11. Reverse Engineering.
12. Reporting Tools.
13. Hardware Hacking [4].

This amount of software is beyond the scope of the educational process. This gives an opportunity for our students, graduate students, and teachers to use this platform for scientific circles and researches and to write bachelor's and master's works, as well as PhD.

Thus, the implementation in the educational process of the State University of Telecommunications innovative technology "Cyber Range" allows to training on the specialty "Cyber Security" at the level of international European standards. The most important is to level up students practical skills in cyber protection of information systems in accordance with world standards.

References:

1. Educating the Next generation experts in Cyber Security: the new EU-recognized Master's program. http://engensec.eu/about-the-project/

2. Sokolov, V. Wireless and Mobile Security : Laboratory Workshop / V. Sokolov, M. Taj Dini, V. Buryachok. — K. : SUT, 2017. — 124 p.

3. Соколов, В. Ю. Безпека безпроводових і мобільних мереж : Лабораторний практикум / В. Ю. Соколов, М. Тадж-Діні / ред. перекл. О. П. Райтер. — К. : ДУТ, 2018. — 122 с. [Ukrainian].

4. Kali Linux Tools Listing. https://tools.kali.org/tools-listing

Євгеній Яковенко
Ситуаційний центр протидії кібербатакам СБУ
Київ, Україна

КІБЕРНЕТИЧНІ АТАКИ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Основним завданням Ситуаційного центру протидії кіберзагрозам є створення умов для безпечного функціонування кіберпростору, його використання в інтересах суспільства і держави - забезпечення кіберзахисту державних електронних інформаційних ресурсів, боротьба з кібертероризмом та кібершпигунством, а також реагування на комп'ютерні інциденти у сфері державної безпеки.

Протягом 2017 року Ситуаційним центром протидії кіберзагрозам виявлено та попереджено проведення спеціальними службами Російської Федерації низки цілеспрямованих кібернетичних атак направлених на отримання доступу до інформації, що обробляється в інформаційних системах органів державної влади України, а також проведення акцій технологічного (кібернетичного) тероризму, спрямованих на порушення штатного режиму функціонування комп'ютерних мереж та систем керування технологічними процесами на об'єктах критичної інфраструктури нашої держави.

Співробітники Ситуаційного центру протидії кіберзагрозам приймали безпосередню участь у розслідуванні більшості кібератак щодо державних електронних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури України.

Ключовими функціями Центру є запровадження системи виявлення та реагування на кібератаки та лабораторії з комп'ютерної криміналістики. За підтримки міжнародної спільноти в Україні буде створено мережу ситуаційних центрів кібербезпеки. Принциповим аспектом роботи Центру СБУ є його відкритість для співпраці з міжнародними установами, організаціями, підприємствами та профільними фахівцями.

Бойові дії у кіберпросторі становлять важливий елемент гібридної війни проти України. Кількість кібератак з ознаками участі спецслужб Росії невпинно зростає протягом 2014-2018 років. При чому, їх проведення направлено на викрадення інформації в органах державної влади України, блокування роботи підприємств соціальної сфери, нанесення фінансової та матеріальної шкоди державним інституція, розміщення недостовірної інформації з метою дискредитації уряду.

Так, у 2014 році кібершпигунські напади здійснено на комп'ютерні мережі Центральної виборчої комісії, Міністерства закордонних справ, Посольств України у Литві, Естонії, Бельгії, Місії України при НАТО. У 2015 року зловмисниками викрадалась інформація з комп'ютерів співробітників правоохоронних органів, Збройних Сил та учасників АТО.

Проте, на рубежі 2015 і 2016 років деструктивним програмним забезпеченням виведено з ладу комп'ютерні мережі енергетичних підприємств Київської, Хмельницької, Івано-Франківської, Чернівецької областей, внаслідок чого без електропостачання залишилось декілька десятків тисяч споживачів цих регіонів України. У грудні 2016 року відбулось декілька послідовних потужних кібератак на важливі об'єкти економіки, енергетики і транспорту України.

Так, 6 грудня атаковано Державне казначейство та Міністерство фінансів, 14 грудня – публічне товариство "Укрзалізниця". 17 грудня внаслідок кібератаки виведено з ладу електропідстанцію "Північна" Національної енергетичної компанії "Укренерго". 20 грудня