© Buryachok V., Bogush V. Guidelines for the development and implementation training profile «cyber security» in Ukraine // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 126-131.

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

РЕКОМЕНДАЦІЇ ЩОДО РОЗРОБКИ ТА ЗАПРОВАДЖЕННЯ ПРОФІЛЮ НАВЧАННЯ «КІБЕРНЕТИЧНА БЕЗПЕКА» В УКРАЇНІ

Володимир Бурячок, Володимир Богуш

Державний університет телекомунікацій, Україна

БУРЯЧОК Володимир Леонідович, д.т.н.

Рік та місце народження: 1963 рік, м. Лутугіно Луганської обл., Україна
Освіта: Київське Вище інженерне радіотехнічне училище ППО, 1985 рік
Посада: завідуючий кафедрою інформаційної та кібернетичної безпеки з 2013 року
Наукові інтереси: системний аналіз, математичне моделювання та програмування; прийняття рішень та науково-технічне прогнозування; нові досягнення в галузі інформаційних технологій; теорія і практика інформаційної та кібернетичної безпеки
Публікації: більше 140 наукових публікацій, серед яких наукові статті у міжнародних та вітчизняних фахових журналах, підручники, монографії, тези доповідей на наукових конференціях і семінарах
E-mail: ikb.dut.edu.ua@gmail.com

БОГУШ Володимир Михайлович, к.т.н.

Рік та місце народження: 1949 рік, с. Стоянів Радехівського р-ну Львівської обл., Україна
Освіта: Київське Вище інженерне радіотехнічне училище ППО, 1972 рік
Посада: професор кафедри інформаційної та кібернетичної безпеки з 2013 року
Наукові інтереси: теорія і практика національної та інформаційної безпеки; безпека кібернетичного простору
Публікації: більше 80 наукових публікацій, серед яких наукові статті у фахових журналах, підручники, монографії, винаходи, тези доповідей на наукових конференціях та семінарах
E-mail: ikb.dut.edu.ua@gmail.com

Анотація. *Розвиток інформаційних та комунікаційних технологій спричинив глибокі системні перетворення в інформаційному та кібернетичному просторах. Останній, в силу своєї специфіки, породжує нові загрози та виклики фахівцям з інформаційної безпеки. Традиційні фахівці з інформаційної безпеки зіштовхуються з новими специфічними завданнями, які вимагають від них нових знань та вмінь. З огляду на це, у роботі, для забезпечення потреб силових структур, а також виробничої та банківської сфери України у фахівцях, спроможних виявляти ознаки та активно протидіяти сторонньому кібернетичному впливу, авторами пропонується підхід до запровадження в системі вищої освіти України профілю навчання «кібернетична безпека». Крім того, чітко визначено критерії, яким мають відповідати такі фахівці.*

Ключові слова: *кібератака, кібервплив, кібербезпека, кіберпростір, інформаційно-комунікаційні технології, підготовка фахівців.*

Вступ

Науково-технічна революція наприкінці XX початку XXI сторіччя спричинила у світі глибокі системні перетворення. Вони, як результат, дали можливість завдяки синтезу перспективних інформаційно-комунікаційних технологій (ІКТ) і бурхливого розвитку інформаційно-телекомунікаційних систем (ІТС) сформуватись та розвинутись принципово новим глобальним субстанціям – інформаційному суспільству, а також інформаційному і кібернетичному просторам, які мають нині практично необмежений потенціал і

відіграють суттєву роль в економічному та соціальному розвитку будь-якої країни світу. Разом з цим неконтрольоване поширення і використання ІКТ та ІТС призвело до того, що світова спільнота отримала не тільки значні переваги, а й цілу низку проблем – передусім значну уразливість власної інфосфери від стороннього кібернетичного впливу. Це визначило політичну необхідність контролю і подальшого регулювання взаємовідносин у цій царині та дало підстави стверджувати про особливу актуальність процесу створення надійної системи кібернетичної безпеки (*стану захищеності кіберпростору держави в цілому або окремих об'єктів його інфраструктури від ризику стороннього кібернетичного впливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним та/або національним інтересам)*, відсутність якої може призвести до втрати політичної незалежності будь-якої держави світу, тобто до фактичного програшу нею війни невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони [1, 2].

Мета роботи полягає у визначені критеріїв, яким мають відповідати фахівці з кібернетичної безпеки та сформувати рекомендації для запровадження у системі вищої освіти України відповідного профілю навчання.

Основна частина

Характерними ознаками, які нині уособлюють поняття кібербезпеки, є сукупність активних захисних і розвідувальних дій (рис. 1), що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо інформаційного ресурсу (ІР), ІКТ і ІТС [3].

Рис. 1. Складові кібернетичної безпеки

Такі дії спрямовані на досягнення і утримання потенційними протиборчими сторонами переваги у протидії новим загрозам безпеці для власних об'єктів критично важливої фізичної, інформаційної та кіберінфраструктури (рис. 2). Зважаючи, що саме це останнім часом відіграє важливу роль у геополітичній конкуренції переважної більшості країн світу, забезпечення кібербезпеки та миру у кіберпросторі стає найбільш важливим завданням нашої інформаційної епохи [4, 5].

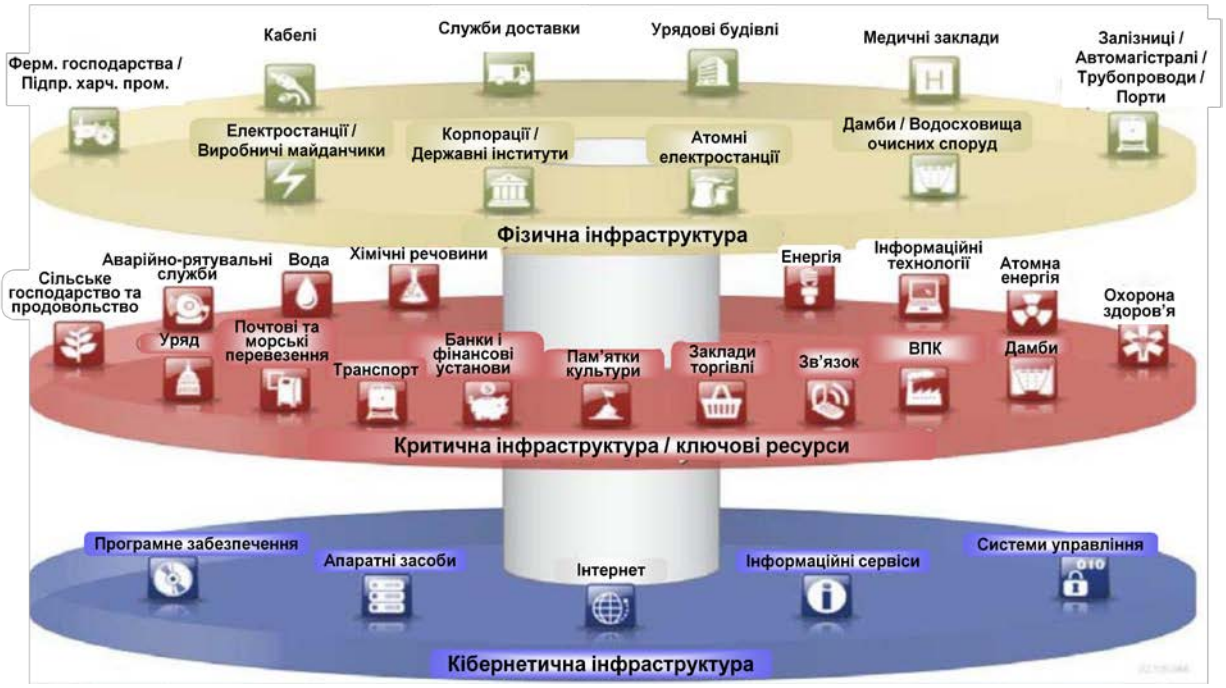

Рис. 2. Критично важливі складові фізичної, інформаційної та кіберінфраструктур

Впродовж останніх років Україна робить певні кроки у напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кіберзлочинністю. Нормативно-правову базу у цих сферах діяльності складає:

Конвенція Ради Європи про кіберзлочинність [6], ратифікована Законом України від 7.09.2005 року № 2824-IV;

Закони України «Про інформацію» [7], «Про основи національної безпеки України» [8], «Про Державну службу спеціального зв'язку та захисту інформації України» [9], «Про телекомунікації» [10],

«Про захист інформації в інформаційно-телекомунікаційних системах» [11], «Про доступ до публічної інформації» [12], «Про оборону України» [13], «Про засади внутрішньої і зовнішньої політики» [14], «Про об'єкти підвищеної небезпеки» [15];

Укази Президента України, зокрема про: Доктрину інформаційної безпеки [16], Стратегію національної безпеки України [17] та Воєнну доктрину України [18];

окремі положення Кримінального Кодексу України, окремі Постанови Кабінету Міністрів та Рішення РНБО України.

При цьому ключова роль у забезпеченні кібербезпеки покладається на:

1) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та IT систем;

2) Закон України «Про Основні засади розвитку інформаційного суспільства України на 2007-2015 роки» [19] у запропонованих змінах до якого указується на необхідність створення національної системи кібербезпеки;

3) запропонований Міністерством внутрішніх справ (МВС) законопроект «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» [20], яким має бути запроваджено низку термінів, пов'язаних із кібербезпекою.

Практичними кроками щодо реалізації існуючої нормативно-правової бази стало створення у 2007 році в складі Державної служби спеціального зв'язку та захисту інформації України Центру реагування на комп'ютерні інциденти. На виконання статті 35 Конвенції про кіберзлочинність у червні 2009 року при Службі безпеки (СБ) України на базі спеціального підрозділу для боротьби з кіберзагрозами утворено Національний контактний пункт формату 24/7 щодо реагування та обміну терміновою інформацією про вчинені кіберзлочини. Окрім цього Указом Президента України «Про виклики та загрози національній безпеці України у 2011 році» від 10 грудня 2010 року №1119/2010 ухвалено рішення щодо початку створення Єдиної загальнодержавної системи протидії кіберзлочинності. Іншим Указом Президента України «Про внесення змін до деяких законів України про структуру і порядок обліку кадрів Служби безпеки України» від 25 січня 2012 року №34 у структурі СБ України створено Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. Усвідомлюючи ступінь та динаміку поширення комп'ютерних інцидентів теренами України у липні 2010 року в структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми утворено новий структурний підрозділ – Департамент боротьби з кіберзлочинністю і торгівлею людьми.

Проте у аналітичній доповіді Національного інституту стратегічних досліджень при Президенті України «Кібербезпека: світові тенденції та виклики для України» [21] зазначається про «незадовільне кадрове забезпечення відомств відповідними фахівцями у сфері інформаційної безпеки», незважаючи на те, що ціла низка вищих навчальних закладів України здійснює підготовку фахівців за різноманітними спеціальностями галузі знань 1701 «Інформаційна безпека». Аналіз недавно введених галузевих стандартів вищої освіти у галузі знань 1701 Інформаційна безпека, зокрема, освітньо-кваліфікаційної характеристики (ОКХ) [22] та освітньо-професійної програми (ОПП) [23] за напрямом 6.170101 «Безпека інформаційних і комунікаційних систем» і показує, що професійні компетентності, задекларовані в цих галузевих стандартах, недостатньо враховують стан та перспективу розвитку методів та засобів забезпечення кібернетичної безпеки. Тому проблема побудови профілю навчання бакалаврів, спеціалістів і магістрів щодо кібернетичної безпеки відповідно до найновіших досягнень у галузі розбудови кібернетичного простору та забезпечення кібернетичної безпеки вважається авторам надзвичайно актуальною.

Більш детально зупинимось на підготовці відповідно до потреб реального сектору економіки фахівців із захисту інформації в інформаційно-комунікаційних системах за напрямом підготовки 6.170101 - «Безпека інформаційних і комунікаційних систем». У сучасних умовах область професійної діяльності такого фахівця включає, як відомо, сфери науки, техніки й технології, що охоплюють сукупність проблем, пов'язаних із забезпеченням не тільки інформаційної, а і кібернетичної безпеки, а також захищеності інформаційного і кіберпросторів держави в цілому або окремих об'єктів їх інфраструктури від ризику стороннього кібернетичного впливу [24-26]. Об'єктами його професійної діяльності при цьому є:

– об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні й інформаційно-аналітичні системи, інформаційні ресурси й інформаційні технології в умовах існування кіберзагроз в інформаційній сфері;

– технології забезпечення кібербезпеки об'єктів різного рівня (система, об'єкт системи, компонент об'єкта), які пов'язані з інформаційними технологіями, використовуваними на цих об'єктах;

– процеси управління інформаційною і кібербезпекою об'єктів, що захищаються.

Враховуючи таке у варіативній частині існуючих навчальних планів підготовки таких фахівців, які регламентуються нині галузевими стандартами вищої освіти України (рис. 3) [22, 23], слід передбачити можливість викладання низки, наприклад, таких дисциплін:

«Кібернетичний простір»;

«Інформаційні технології та системи кібернетичного простору»;

«Технологія організації збору та добування інформації у кіберпросторі, її обробки аналізу і синтезу»;

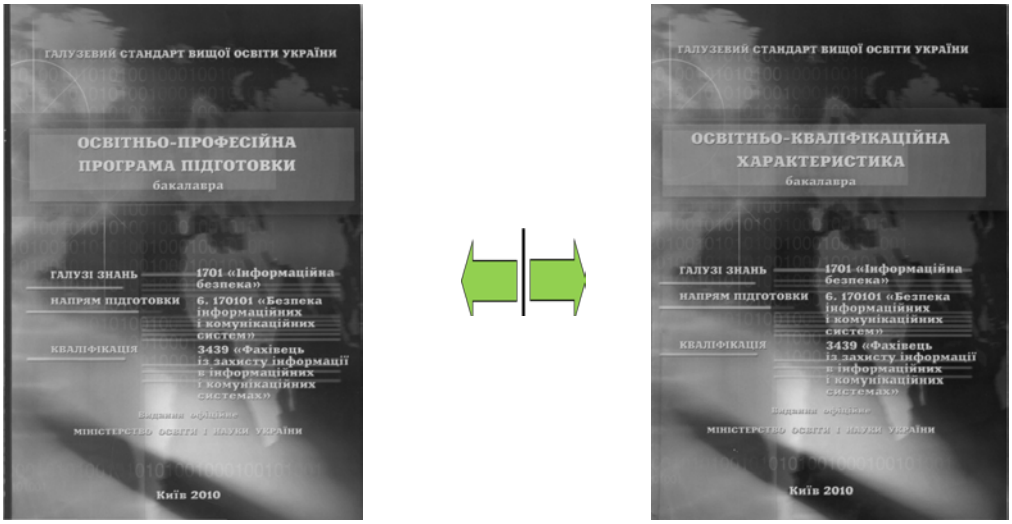

Рис. 3. Стандарти вищої освіти України за галуззю знань «Інформаційна безпека»

«Основи автоматизації процесів інформаційної діяльності у кібернетичному просторі».

Це дасть змогу сформувати базис у виді *компетенцій* (соціально-особистісних, інструментальних, загальнонаукових та професійних), *виробничих функцій* (дослідницьких, проектувальницьких, організаційних, управлінських, технологічних, контрольних, прогностичних та технічних) та типових задач, що ним відповідають, а також *умінь*, якими має володіти випускник-бакалавр та фактично закласти фундамент для підготовки професіоналів із організації кібернетичної безпеки за спеціальностями 7.17010101 та 8.17010101 – «Безпека інформаційних і комунікаційних систем».

Наступним, а реально кроком практично паралельним першому, має стати впровадження у варіативних частинах існуючих навчальних планів підготовки спеціалістів і магістрів у цій сфері діяльності таких дисциплін, які розглядатимуть питання, пов'язані із протидією кіберзлочинності та забезпеченням кібербезпеки особистості, підприємства та держави у цілому. Найбільш цікавими з точки зору майбутніх працедавців можуть стати знання, які стосуються:

– теоретичних основ кібернетичної безпеки;

– правових та організаційних засад протидії кіберзлочинності;

– методів та засобів протидії кіберзлочинності;

– програмного забезпечення систем кібернетичної безпеки;

– криптографічних механізмів кібернетичної безпеки;

– кібернетичної безпеки підприємств;

– основ кібернетичної безпеки держав тощо.

Такий підхід до появи нових стандартів вищої освіти України, які б регламентували галузеві кваліфікаційні вимоги до соціально-виробничої діяльності випускника ВНЗ за напрямом 6 (7, 8).170101 – «БІКС» з урахуванням положень щодо кібернетичної безпеки та державні вимоги до властивостей і якостей особи яка здобула вищу освіту цього напряму, визначали нормативний термін і зміст навчання та нормативні форми державної атестації, а також встановлювали вимоги до змісту, обсягу й рівня освіти та професійної підготовки такого випускника дозволить сформувати у нього такі основні компетенції:

– здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства, застосовувати досягнення інформатики й обчислювальної техніки, проводити цілеспрямований пошук і збір інформації з відкритих, а також її добування з відносно-відкритих і закритих електронних джерел;

– здатність виявляти ознаки стороннього кібернетичного впливу, а також моделювати можливі ситуації такого впливу та прогнозувати їх можливі наслідки;

– здатність організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної і кібербезпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізуємості й економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації;

– здатність протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ систем і мереж, забезпечити стійкість їх роботи, а також відновлення їх нормального функціонування після здійснення кібернападів;

– здатність організовувати проведення атестації об'єкта на відповідність вимогам державних або корпоративних нормативних документів;

– здатність брати участь у розробці підсистем управління інформаційною і кібербезпекою, здійснювати їх адміністрування й експлуатацію;

– здатність до проведення попереднього техніко-економічного аналізу й обґрунтування проектних рішень по забезпеченню кібербезпеки;

– здатність оформлювати технічну документацію з урахуванням діючих нормативних і методичних документів в області інформаційної і кібербезпеки;

– здатність до програмної реалізації алгоритмів рішення типових завдань забезпечення інформаційної і кібербезпеки й до застосування програмних засобів системного, прикладного й

спеціального призначення;

− здатність проводити аналіз інформаційної безпеки об'єктів і систем з використанням вітчизняних і закордонних стандартів;

− здатністю формувати комплекс мір (правила, процедури, практичні прийоми та ін.) для керування інформаційною і кібербезпекою тощо.

Висновки

Як результат слід наголосити, що фахова підготовка фахівців з інформаційної і кібербезпеки та керівного складу органів державного управління з цих питань для потреб як силових структур, так і виробничої та банківської сфери має проводитись у єдиній системі освіти України, а спеціальна підготовка офіцерського складу ЗС України та інших силових структур із загальних питань інформаційної і кібербезпеки має проводитись у системі командирської підготовки та на курсах підвищення кваліфікації.

Література

[1] A Solution-based Examination of Local, State, and National Government Groups Combating Terrorism and Cyberterrorism. By: Matusitz, Jonathan; Breen, Gerald-Mark. Journal of Human Behavior in the Social Environment, Feb2011, Vol. 21 Issue 2, p. 109-129, 21 p. [Електронний ресурс]. – Режим доступу: http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN.

[2] Руководство по кибербезопасности для развивающихся стран. [Електронний ресурс]. – Режим доступу: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-r.pdf.

[3] Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.

[4] National Strategy to Secure Cyberspace. U.S. government via Department of Homeland Security. February 2003. p. 16. Retrieved 2008-05-18. [Електронний ресурс]. – Режим доступу: ttp://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

[5] ITU's Global Cybersecurity Agenda: An International Framework for Cybersecurity. - Geneva : ITU, 2007. - 46 pp.. [Електронний ресурс]. – Режим доступу: http://www.itu.int/osg/csd/cybersecuritv/gca/index.html.

[6] Про ратифікацію Конвенції про кіберзлочинність: за станом на 14.10.2010 р. / Закон, затверджений ВР України 07.09.2005, № 284-IV. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2824-15. Офіц. вид. – К.: Відомості Верховної Ради України від 10.02.2006.

[7] Про інформацію: за станом на 09.05.2011 р. / Закон, затверджений ВР України 02.10.1992, № 2657-XII. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Відомості Верховної Ради України від 01.12.1992.

[8] Про основи національної безпеки України: за станом на 20.07.2010 р. / Закон, затверджений ВР України 19 червня 2003 р., № 964-IV. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Урядовий кур'єр від 30.07.2003, № 139.

[9] Про державну службу спеціального зв'язка та захисту інформації: за станом на 07.08.2011 р. / Закон, затверджений ВР України 23 лютого 2006 року, № 3475-IV. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Урядовий кур'єр від 11.04.2006, № 68.

[10] Про телекомунікації: за станом на 15.10.2011 р. / Закон, затверджений ВР України, 18.11.2003, № 1280-IV. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Урядовий кур'єр від 24.12.2003, № 243.

[11] Про захист інформації в інформаційно-телекомунікаційних системах: за станом на 30.04.2009 р. / Закон, затверджений ВР України 05.07.1994, № 80/94-ВР. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Відомості Верховної Ради України від 02.08.1994.

[12] Про доступ до публічної інформації: за станом на 09.06.2013 р. / Закон, затверджений ВР України 13.01.2011, № 2939-VI. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2939-17. – Офіц. вид. – К.: Відомості Верховної Ради України від 12.08.2011.

[13] Про оборону України: за станом на 01.07.2013 р. / Закон, затверджений ВР України 06.12.1991, № 1932-XII. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1932-12. – Офіц. вид. – К.: Відомості Верховної Ради України від 03.03.1992.

[14] Про засади внутрішньої і зовнішньої політики: за станом на 01.07.2010 р. / Затве Закон, затверджений рджений ВР України 01.07.2010, № 2411-VI. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2411-17. – Офіц. вид. – К.: Відомості Верховної Ради України від 08.10.2010.

[15] Про об'єкти підвищеної небезпеки: за станом на 18.11.2012 р. / Закон, затверджений ВР України 18.01.2001, № 2245-III. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2245-14. – Офіц. вид. – К.: Відомості Верховної Ради України від 13.04.2001.

[16] 16. Про Стратегію національної безпеки України: за станом на 12.02.2007 р. / Указ Президента України від 12.02.2007 р., № 105/2007. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/ main.cgi. – Офіц. вид. – К.: Урядовий кур'єр від 07.03.2007, № 43.

[17] Про Доктрину інформаційної безпеки України: за станом на 08.07.2009 р. / Указ Президента

України від 8.02.2009 р., № 514/2009. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/ main.cgi. – Офіц. вид. – К.: Офіційний вісник України від 20.07.2009.

[18] Про Воєнну доктрину України: за станом на 22.06.2012 р. / Указ Президента України від 15.06.2004, № 648/2004. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/648/2004. – Офіц. вид. – К.: Офіційний вісник України від 13.08.2004.

[19] Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: за станом на 09.01.2007р. / Закон, затверджений ВР України 09.01.2007 № 537-V. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/537-16. – Офіц. вид. – К.: Відомості Верховної Ради України від 23.03.2007.

[20] Про внесення змін до Закону України "Про основи національної безпеки України" щодо кібернетичної безпеки України: проект за станом на 06.03.2013 р. № 2483. [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998.

[21] Дубов Д.В. Кібербезпека: світові тенденції та виклики для України. Аналітична доповідь. / Д.В. Дубов, М.А. Ожеван. – К.: НІСД, 2011. – 30 с.

[22] Галузевий стандарт вищої освіти України з галузі знань 1701 Інформаційна безпека за напрямом підготовки бакалавра 6.170101 Безпека інформаційних і комунікаційних систем. Освітньо-кваліфікаційна характеристика. Затверджений Наказом Міністерства освіти і науки України 9 липня 2010 р. № 687.

[23] Галузевий стандарт вищої освіти України з галузі знань 1701 Інформаційна безпека за напрямом підготовки бакалавра 6.170101 Безпека інформаційних і комунікаційних систем. Освітньо-професійна програма підготовки. Затверджений Наказом Міністерства освіти і науки України 9 липня 2010 р. № 687.

[24] Сисоєв В. Аналіз рівня освіти та підготовки фахівців з управління IT та інформаційної безпеки в Україні. Режим доступу: http://www.auditagency.com.ua/blog/ISACA_research_ Education.pdf.

[25] Ю. Г. Даник, Ю. М. Супрунов. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України. Збірник наукових праць ЖВІ НАУ «Інформаційні системи». Випуск 5. 2011. С.5-22

[26] Міночкін А. І. Інформаційна боротьба: сучасний стан та досвід підготовки фахівців / А. І. Міночкін // Оборонний вісник. – К. : Центр воєнної політики та політики безпеки, 2011. – № 2. – С. 12–14.

УДК 004.056.5:378.1 (045)

Бурячок В.Л., Богуш В.М. Рекомендации по разработке и введению профиля обучения «кибернетической безопасности» в Украине

Аннотация. *Развитие информационных и коммуникационных технологий вызвало глубокие системные преобразования в информационном и кибернетическом пространствах. Последний, в силу своей специфики, порождает новые угрозы и вызовы специалистам по информационной безопасности. Традиционные специалисты по информационной безопасности сталкиваются с новыми специфическими задачами, которые требуют от них новых знаний и умений. Учитывая это, в работе, для обеспечения потребностей силовых структур, а также производственной и банковской сферы Украины в специалистах, способных выявлять признаки и активно противодействовать постороннему кибернетическому влиянию, авторами предлагается подход к внедрению в системе высшего образования Украины профиля обучения «кибернетическая безопасность». Кроме того, четко определены критерии, которым должны соответствовать такие специалисты.*

Ключевые слова: *кибератака, кибервлияние, кибербезопасность, киберпространство, информационно-коммуникационные технологии, подготовка специалистов.*

Buryachok V., Bogush V. Guidelines for the development and implementation training profile «cyber security» in Ukraine

Abstract. *The development of information and communication technologies has caused profound systemic changes in the information space and cyberspace. Cyberspace, by virtue of their nature, creates new threats and challenges for information security professionals. Traditional information security professionals face new specific tasks that require them to new knowledge and skills. In view of this, the paper to meet the needs of law enforcement agencies, as well as industrial and banking professionals in Ukraine capable of detecting signs and actively counteract cybernetic an outside influence, the authors suggest an approach to the introduction of higher education in Ukraine learning profile «cyber security». In addition, in the paper clearly defined criteria to be met by such specialists.*

Key words: *cyberattack, cyber influence, cybersecurity, cyberspace, information & communication technology, training.*

Отримано *17 квітня 2014 року*, затверджено редколегією *20 травня 2014 року*