DOI: 10.18372/2410-7840.20.12862
УДК 004.056

РЕКОМЕНДАЦІЇ ЩОДО РОЗРОБКИ ТА РЕАЛІЗАЦІЇ МОДЕЛІ ПРОФЕСІЙНИХ КОМПЕТЕНТНОСТЕЙ У СФЕРІ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

Володимир Бурячок, Володимир Богуш

У статті проаналізовано формування інформаційного та кіберпросторів і, як результат, зроблено висновок про посилення інформаційної конфронтації між країнами та їх вступ до якісно нової фази взаємовідносин – інформаційного та кіберпротиборства. Такий стан справ вимагає якісного нового підходу до підготовки ІТ фахівців, з орієнтуванням її передусім на практичну площину в сфері інформаційної і кібернетичної безпеки. Для вирішення цього завдання в статті визначено найбільш пріоритетні ключові напрямки підготовки таких фахівців. На основі результатів аналізу законодавства України щодо кібербезпеки та типового навчального плану НАТО з кібербезпеки запропоновано певну модель щодо підготовки фахівців для національної системи кібербезпеки. Імплементовані в моделі компетентності та результати навчання можуть бути покладені в основу розробки освітніх програм та навчальних планів якісної підготовки фахівців для національної системи кібербезпеки, а саме бакалаврів з кібербезпеки за погодженим у 2017 році Національним агентством із забезпечення якості вищої освіти стан-дартом, а також створення нових стандартів стосовно кібербезпеки на наступних освітньо-професійному та освітньо-науковому рівнях. В статті запропоновано декілька основних класів моделі професійних компетентностей у сфері підготовки фахівців для національної системи кібербезпеки. Зважаючи, що основними суб'єктами національної системи кібербезпеки відповідно до Конституції та законів України є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи та Національний банк України, в роботі запропоновано узгоджені з покладеними на ці структури завданнями, моделі професійних компетентностей для підготовки їх особового складу.

Ключові слова: *інфраструктура, кібербезпека, кіберзагроза, кібероборона, кіберпростір, компе-тентність, система*

Вступ і постановка задачі

Людству (за оцінками) біля 60 тисяч років. За цей час змінилося понад 1800 поколінь, але лише одному з них в цей період властивою виявилась так звана інформаційна глобалізація. Її виникненню у XVIII – XIX ст. сприяли чотири світові індустріальні та одна інформаційна революції, а також винайдення двох простих, але дуже змістовних законів, сформульованих Гордоном Муром та Робертом Меткалфом, які обумовили появу і формування простору інформаційного та кібернетичного. Це, як наслідок:

– по-перше, сприяло формуванню сучасного інформаційного суспільства;

– по-друге, призвело до синтезу двох інформаційно-комунікаційних технологій – інформаційної та телекомунікаційної.

Разом з тим питання щодо міждержавного паритету та взаємовідносин в інформаційному і кіберпросторах, на відміну від таких просторів, як наземний, морський, повітряний та космічний й нині залишаються відкритими й такими, що потребують свого розв'язку. Такий стан справ пояснюється передусім безпрецедентним впливом на сучасне суспільство, інформаційний та кіберпростори низки інформаційних та кібероперацій, які для переважної більшості держав земної кулі останнім часом стали невід'ємною частиною їх внутрішньої і зовнішньої політики, відіграють суттєву роль в їх економічному і соціальному розвитку та свідчать про їх вступ до якісно нової фази взаємовідносин – інформаційного та кіберпротиборства.

Поряд з вибуховим зростанням обсягів даних, до яких отримали доступ пересічні громадяни та їх переходом в хмару, а також винайденням потужних комп'ютерів та вбудованих мікроконтролерів це спонукає країни світу не тільки до глобальної інтелектуалізації та отриманню певних переваг, але й сприяють виникненню низки проблем – передусім безпекового характеру, роблячи більш вразливими перш за все критично-важливі об'єкти інфраструктури цих країн до загроз антропогенного і техногенного характеру та природних катаклізмів. Про це було офіційно заявлено на Всесвітньому економічному форумі, що проходив у Давосі в січні 2017 й, як наслідок, констатовано про політичну необхідність контролю та подальшого регулювання взаємовідносин у цих царинах, а також про особливу актуальність процесу створення країнами світу власних систем безпеки, які в най

ближчій перспективі відіграватимуть надзвичайно важливу роль у міжнародній геополітичній конкуренції. Це, в свою чергу, потребує нового підходу до підготовки відповідних фахівців, здатних у стислі терміни реагувати на кіберінциденти та протидіяти кіберзагрозам, проводити аудити стану інформаційної та кібербезпеки (ІКБ), створювати ефективні системи управління ІКБ тощо [1]. Саме це й обумовлює **актуальність** теми. Дослідженням зазначених проблем протягом останніх років займались як вітчизняні – Ю.Г. Даник, Д.В. Дубов, А.І. Міночкин, В.А. Сисоєв, Ю.М. Супрунов та інші, так і закордонні фахівці.

Мета роботи полягає у виробленні пропозицій щодо коригування моделі компетентностей, які можуть бути покладені в основу розробки освітніх програм та навчальних планів для якісної підготовки бакалаврів з кібербезпеки за погодженим у 2017 році Національним агентством із забезпечення якості вищої освіти стандартом [2], а також створення нових стандартів стосовно кібербезпеки на наступних освітньо-професійному та освітньо-науковому рівнях.

Новизна дослідження обумовлюється спробою формування на підставі типового навчального плану НАТО з кібербезпеки та компетентностей і результатів навчання, визначених вітчизняною нормативно-правовою базою [2], сучасну модель підготовки фахівців для національної системи кібербезпеки.

Виклад основного матеріалу дослідження. Передумовою вирішення цього завдання є результати прогнозу щодо глобальної трансформації компетентностей на найближчі 4-5 років, що належать аналітикам World Economic Forum, а також основні положення типового навчального плану з кібербезпеки, розробленого у 2017 році робочою групою консорціуму «Партнерство заради миру» [3]. Головними компетентностями в осяжному майбутньому, як вважає міжнародна спільнота, будуть:

- вміння вирішувати складні задачі;
- вміння критично мислити;
- вміння бути креативним;
- вміння управляти людьми;
- навички до координації та взаємодії;
- навички емоційного інтелекту;
- вміння приймати рішення;
- навички орієнтування на клієнта;
- вміння вести перемовини;
- навички когнітивної гнучкості.

Разом з цим, як в процесі коригування моделі компетентностей на бакалаврському рівні, так й у ході створення нових стандартів з кібербезпеки на магістерському рівні та рівні підготовки докторів філософії, слід прийняти до уваги, що за аналогією з класичним визначенням інформаційної безпеки під кібербезпекою фактично розуміють властивість захищеності активів від загроз конфіденційності, цілісності, доступності, але в деяких абстрактних рамках – кіберпросторі (рис. 1) [4].

Що стосується власне забезпечення кібербезпеки, то в якості пріоритету доцільно виділити координацію взаємодії між організаціями, що формують кіберпростір, самостійні дії яких не забезпечують ефективний захист від кіберзагроз. Прикладна галузь кібербезпеки (рис. 2) є інтегрованою з поняттями інформаційної безпеки (ІБ), безпеки застосувань, мережної безпеки, безпеки глобальної мережі, а також безпеки критичної інформаційної інфраструктури.

При цьому: безпека застосувань визначається у відношенні програмних засобів, а також інформаційно-програмних ресурсів і процесів, що беруть участь в їх життєвому циклі; безпека мереж пов'язана з проектуванням, впровадженням і використанням мереж всередині організації, між організаціями, між організаціями і користувачами; безпека в глобальній мережі стосується послуг мережі та відповідних систем інформаційно-комунікаційних технологій і мереж; безпека критичної інформаційної інфраструктури характеризує захищеність від відповідних загроз, в тому числі загроз ІБ.

Сам процес забезпечення кібербезпеки ґрунтується на ризик-орієнтованому підході, для чого визначаються активи кіберпростору і зацікавлені сторони, загрози, рекомендації і заходи з оброблення ризиків, причому як специфічна міра застосовуються вказівки щодо координації дій та обміну інформацією. Для вирішення завдань раціонального поводження з ризиками організації, що мають вихід у кіберпростір, повинні впровадити у себе систему управління інформаційною безпекою, ключовим фактором у реалізації якої є забезпечення гарантій того, що в організації існує і функціонує система безперервної ідентифікації, оцінювання, обробки та моніторингу ризиків, пов'язаних з її діяльністю, включаючи безпосереднє надання послуг в глобальній мережі кінцевим користувачам або абонентам.

При створенні системи управління інформаційною безпекою в організації необхідно передбачити механізми відстеження і обробки інцидентів безпеки, а також координації заходів реагування на інциденти з підрозділами CIRT, CERT, або CSIRT в державі. Заходи реагування на інциденти повинні передбачати, крім усього іншого, моніторинг та оцінювання рівня безпеки сервісів організації, які використовується кінцевими користувачами, а також надання такої підтримки зацікавленим сторонам, яка буде підвищувати результативність їх власної реакції на прояви інцидентів безпеки.

У зв'язку з наведеним вище можна визначити, наприклад, відповідно до типового навчального плану з кібербезпеки [3], декілька основних класів моделі професійних компетентностей у сфері підготовки фахівців для національної системи кібербезпеки.

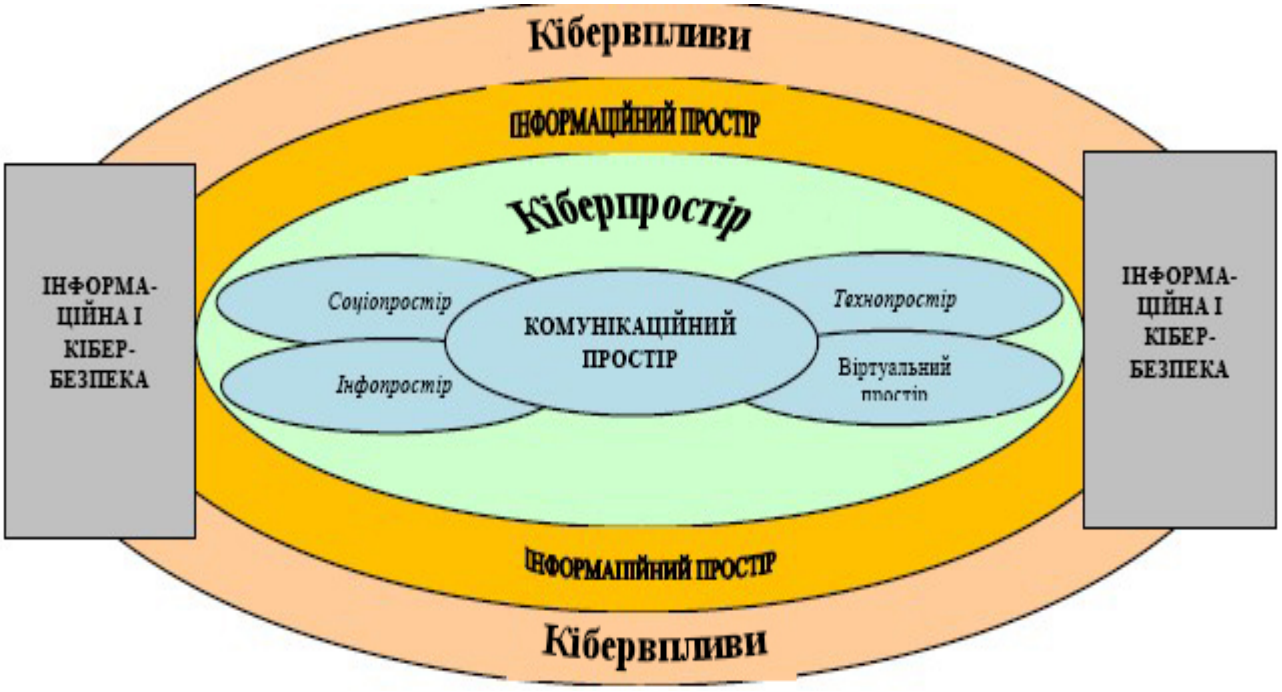

Рис. 1. Взаємозв'язок понять безпека, інформаційний та кіберпростір

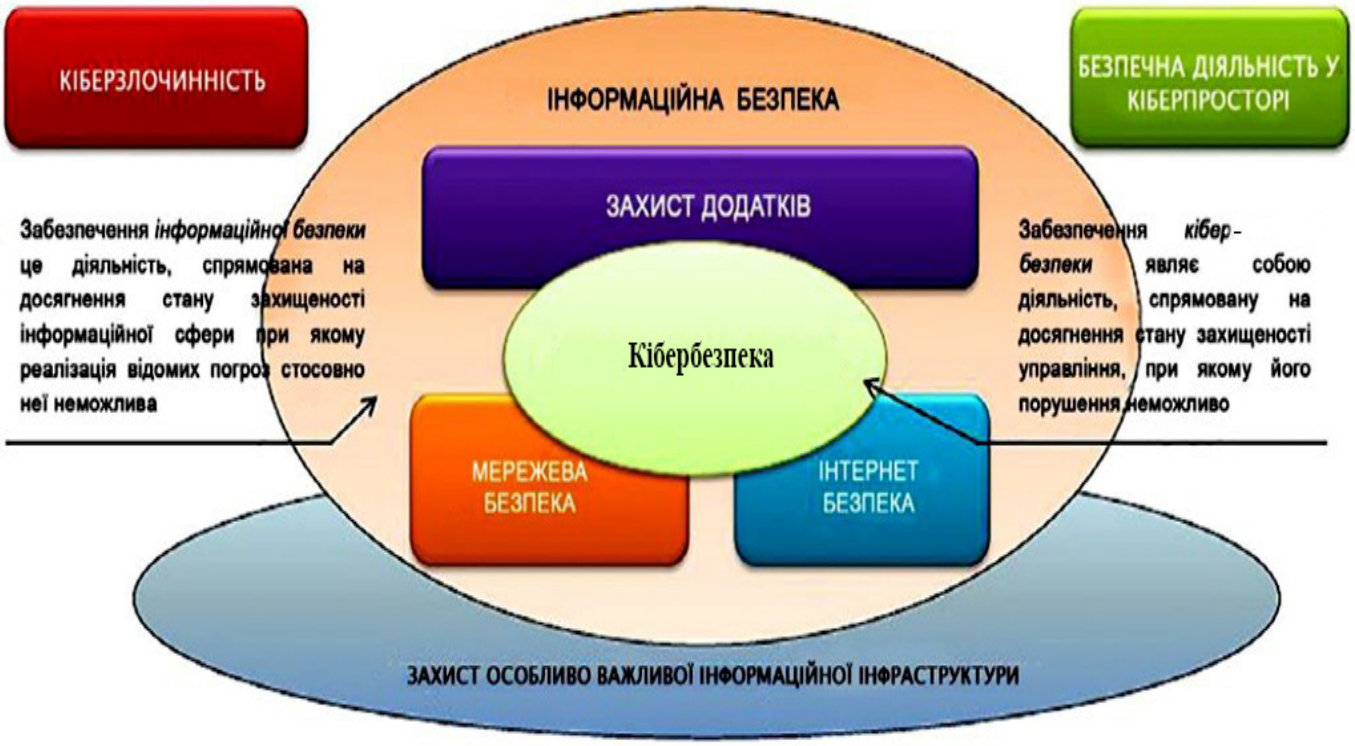

Рис. 2. Прикладна галузь інформаційної та кібербезпеки

До першого класу моделі професійних компетентностей слід віднести такі, що закладають основу наступних класів компетентностей, а також підкласів компетентностей щодо структурних компонентів кіберпростору, його основної архітектури та основ кібербезпеки та архітектури кібербезпеки. Причому компетентності щодо основ ідентифікації ризиків і управління ними повинні бути головним спільним, що зв'язує окремі компетентності і результати навчання.

У зв'язку з цим до другого класу моделі професійних компетентностей повинні входити компетентності щодо уразливостей, характерних для кіберпростору та способів і засобів для використання таких уразливостей за допомогою різних схем або векторів нападу. Розуміння даних уразливостей – невід'ємний компонент ризику і принципів зниження його рівня.

Третій клас професійних компетентностей складають компетентності щодо міжнародних організацій, політики та стандартів у сфері кібербезпеки. Вони полягають у змозі визначити роль організацій за міжнародними стандартами, аналізувати національну політику у сфері кібербезпеки в контексті міжнародних стандартів і рекомендованого досвіду, порівнювати їх з різними прикладами національних принципів, а також міжнародні правові режими кібербезпеки, що знаходяться на стадії розвитку.

До четвертого класу моделі професійних компетентностей можна віднести компетентності у сфері управління кібербезпекою на національному рівні. Це, насамперед, компетентності щодо розуміння методів управління кібербезпекою та рівнем національної готовності у сфері кібербезпеки з контекстом рамок ризику. Це можуть бути:

– компетентності щодо національних методів роботи, принципів дії та організації щодо кіберстійкості, планування в разі виникнення надзвичайних обставин і в процесі відновлення після кіберінцидентів, щоб звести до мінімуму пов'язану з цим дестабілізацію ситуації;

– компетентності щодо національних методів управління кібербезпекою, що включають заходи забезпечення кібербезпеки, реагування на надзвичайні ситуації та мінімізацію ризику;

– компетентності щодо інструментів, методів і процедур у сфері кіберкриміналістики з метою збору, аналізу та інтерпретації даних з метою встановлення атрибуції і для спецслужб;

– компетентності щодо контролю і оцінки безпеки на національному рівні, та оцінки готовності в сфері національної кібербезпеки.

Результати навчання повинні бути наступними:

– здатність до системного знання та викладення методологічних та теоретичних основ забезпечення безпеки особистості, суспільства та держави у кіберпросторі, що включає кібернетичну інфраструктуру, кібернетичні сервіси, соціологічні та психологічні сфери, пов'язані з діяльністю людей;

– володіння достатніми науковими знаннями щодо теоретичних та методологічних основ запобігання кібернетичній злочинності, кібернетичному тероризму, кібернетичним конфліктам і війнам на основі впровадження методів та експлуатації засобів забезпечення кібернетичної безпеки;

– здатність застосовувати стандарти, процедури та додатки для забезпечення конфіденційності, цілісності та доступності інформації та інформаційних систем;

– здатність використовувати системи та інструменти, необхідні для мінімізації ризику у кібернетичному просторі;

– здатність здійснювати організаційно-технічні заходи щодо виявлення загроз й інцидентів, реагування на інциденти та запобігання інцидентам, а також відновлення після інциденту;

– здатність здійснювати розроблення концепцій, проектування та реалізацію системи управління кібербезпекою.

Наведені результати можна прийняти як базові для підготовки фахівців у сфері національної системи кібербезпеки.

Зважаючи, що основними суб'єктами національної системи кібербезпеки відповідно до Конституції та законів України є Державна служба спеціального зв'язку та захисту інформації (ДССЗЗІ) України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи та Національний банк України, - їх особовий склад має бути підготовленим скоріш за все відповідно до моделей професійних компетентностей, які відповідають покладеним на них завданням (рис. 3) [5, 6].

Рис. 3. Розподіл завдань між суб'єктами національної системи кібербезпеки

При цьому, наприклад, для виконання завдань у системі національної системи кібербезпеки ДССЗЗІ України фахівці повинні бути підготовленими відповідно до таких основних професійних компетентностей:

– здатність до формування та реалізації державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, та здійснення державного контролю у цих сферах;

– здатність забезпечувати створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту;

– здійснювати організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків;

– здатність до здійснення інформування про кіберзагрози та відповідні методи захисту від них;

– забезпечення впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлення вимоги до аудиторів інформаційної безпеки, визначення порядку їх атестації (переатестації);

– здатність до координації, організації та проведення аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на уразливість;

– здатність до забезпечення функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

Для виконання завдань у системі національної системи кібербезпеки Національною поліцією України фахівці повинні бути підготовленими відповідно до таких основних професійних компетентностей:

– здатність до забезпечення захисту прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі;

– здатність здійснювати заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі.

Для виконання завдань у системі національної системи кібербезпеки Службою безпеки України фахівці повинні бути підготовленими відповідно до таких основних професійних компетентностей:

– здатність описати широке коло методологічних, наукових та технічних основ побудови кіберпростору;

– здатність описати процеси протиборства у кіберпросторі; здатність аналізувати організацію протиборства у кіберпросторі провідних країн світу;

– здатність аналізувати спеціальні операції у кіберпросторі;

– здатність аналізувати методи та засоби розвідувальної та контррозвідувальної діяльності у кіберпросторі;

– здатність організовувати розвідувальну та контррозвідувальну діяльності у кіберпросторі;

– здатність здійснювати контррозвідувальні та оперативно-розшукові заходи у кіберпросторі.

Для виконання завдань у системі національної системи кібербезпеки Міністерством оборони України, Генеральний штаб Збройних Сил України:

– здатність здійснювати заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони);

– здатність здійснювати військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз;

– впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану.

Для виконання завдань у системі національної системи кібербезпеки розвідувальними органами України фахівці повинні бути здатними до здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Для виконання завдань у системі національної системи кібербезпеки Національним банком України фахівці повинні бути підготовленими відповідно до таких основних професійних компетентностей:

– здатність визначати порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснення контролю за їх виконанням;

– здатність забезпечувати функціонування системи кіберзахисту у банківській системі України;

– здатність забезпечувати проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України.

Висновки

Підготовка фахівців для національної системи кібербезпеки може мати базову основу, що грунтується на компетентностях та результатах навчання, які пропонує стандарт вищої освіти та типовий навчальний план НАТО стосовно кібербезпеки. Підготовка фахівців для складових національної кібербезпеки, які становлять Державна служба спеціального зв'язку та захисту інформа-ції України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, може здійснюватися швидше за все відповідно до моделей професійних компетентностей, що відповідають покладеним на них завданням.

Рекомендації можуть застосовуватися для всіх рівнів підготовки фахівців, включаючи і перепідготовку.

ЛІТЕРАТУРА

[1]. Закон України Про основні засади забезпечення кібербезпеки України. (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) [Електронний ресурс]. Режим доступу: http:// zakon0. rada. gov. ua/ laws/ show/2163-19.

[2]. Перший стандарт вищої освіти стосується кібербезпеки. Нацагентство із забезпечення якості вищої освіти погодило перший стандарт вищої освіти [Електронний ресурс]. Режим доступу: https:// ligazakon.net / lawnews / doc/-NZ173112-PERSHYY- STANDART- VYSHCHOYI-OSVITY-STOSUYETSYA – KIBERBEZPEKY ?type=ep.

[3]. Cybersecurity: A Generic Reference Curriculum (RC). Dear Partners, NATO Members, 4500-1 (OSEM PED) October 2016, 73 p.

[4]. ISO/IEC 27032:2012 Information technology. Security techniques. Guidelines for cybersecurity, 50 p.

[5]. В.Бурячок, В. Богуш, "Рекомендації щодо розробки та запровадження профілю навчання «кібернетична безпека» в Україні", *Ukrainian Scientific Journal of Information Security,* vol. 20, issue 2, pp. 126-131, 2014.

[6]. Ю. Борсуковський, В. Бурячок, "Роль і місце вищих навчальних закладів у створенні системи інформаційної та кібернетичної безпеки України", Сучасний захист інформації №1, С. 34-40, 2017.

РЕКОМЕНДАЦИИ ПО РАЗРАБОТКЕ И РЕАЛИЗАЦИИ МОДЕЛИ ПРОФЕССИОНАЛЬНОЙ КОМПЕТЕНТНОСТИ В СФЕРЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ДЛЯ НАЦИОНАЛЬНОЙ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ

В статье проанализирован процесс формирования информационного и киберпространств и, как результат, сделан вывод об усилении информационной конфронтации между странами и их вхождении в качественно новую фазу взаиных отношений - информационное и кибернетическое противоборство. Это требует качественно нового подхода к подготовке ИТ специалистов, с ориентировкой ее прежде всего на практическую плоскость в сфере информационной и кибернетичнои безопасности. Для решения этой задачи в статье определены наиболее приоритетные ключевые направления подготовки таких специалистов. На основе результатов анализа законодательства Украины по кибербезопасности и типового учебного плана НАТО по кибербезопасности предложена модель подготовки специалистов для национальной системы кибербезопасности. Реализованные в модели компетентности и результаты обучения могут быть положены в основу разработки образовательных программ и учебных планов качественной подготовки специалистов для национальной системы кибербезопасности, а именно бакалавров по кибербезопасности по согласованному в 2017 году Национальным агентством по обеспечению качества высшего образования стандартом, а также создание новых

стандартов относительно кибербезопасности на следующих образовательно-профессиональной и образовательно-научном уровнях. В статье предложено несколько основных классов модели профессиональных компетенций в сфере подготовки специалистов для национальной системы кибербезопасности. Учитывая, что основными субъектами национальной системы кибербезопасности в соответствии с Конституцией и законами Украины является Государственная служба специальной связи и защиты информации Украины, Национальная полиция Украина, Служба безопасности Украины, Министерство оборо-ны Украины и Генеральный штаб Вооруженных Сил Украины, разведывательные органы и Национальный банк Украины, в работе предложены согласованные с возложенными на эти структуры задачами, модели профессиональных компетентностей для подготовки их личного состава.
Ключевые слова: инфраструктура, кибербезопасность, киберугрозы, кибероборона, киберпространство, компетентность, система.

RECOMMENDATIONS FOR DEVELOPMENT AND IMPLEMENTATION OF THE PROFESSIONAL MODELCOMPETENCES IN THE SPHERE OF TRAINING OF SPECIALISTS FOR OF THE NATIONAL CYBER-SECURITY SYSTEM

The article analyzes the process of formation of information and cyberspace, and as a result, a conclusion is made about the intensification of information confrontation between countries and their entry into a qualitatively new phase of mutual relations - information and cybernetic confrontation. This requires a qualitatively new approach to the training of IT professionals, with its orientation primarily on the practical plane in the field of information and cyber-non-security. To solve this problem, the article identifies the most priority key directions for the training of such specialists. Based on the results of the analysis of Ukrainian legislation on cybersecurity and the standard NATO training curriculum on cybersecuri-ty, a model for training specialists for the national cybersecurity system was proposed. The competence and learning out-comes implemented in the model can be used as a basis for the development of educational programs and curricula for qualitative training of specialists for the national cybersecurity system, namely bachelors of cybersecurity, as agreed by the National Agency for Quality Assurance in Higher Education in 2017, new standards on cybersecurity at the following edu-cational-professional and educational-scientific levels. In the article several basic classes of the model of professional com-petencies in the field of training specialists for the national cybersecurity system were proposed. Given that the main sub-jects of the national cybersecurity system in accordance with the Constitution and laws of Ukraine is the State Service for Special Communications and Information Protection of Ukraine, the National Police Ukraine, the Security Service of Ukraine, the Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence bodies and the National Bank of Ukraine, the work agreed upon with the tasks assigned to these structures, models of professional competencies for the preparation of their personal cooperation.
Keywords: infrastructure, cybersecurity, cyberthreats, cyber defense, cyberspace, competence, system.

Бурячок Володимир Леонідович, доктор технічних наук, професор, зав. кафедрою інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка.
E-mail: v.buriachok@kubg.edu.ua.
Бурячок Владимир Леонидович, доктор технических наук, профессор, зав. кафедрой информационной и кибернетической безопасности Киевского университета имени Бориса Гринченко.
Buriachok Volodymyr, Doctor of Technical Sciences, Professor, Head of the Department of Information and cyber security, Borys Grinchenko Kyiv University.

Богуш Володимир Михайлович, кандидат технічних наук, доцент, професор кафедри технічного захисту інформації Національної Академії Служби безпеки України.
E-mail: bogush_vm@ukr.net.
Богуш Владимир Михайлович, кандидат технических наук, доцент, профессор кафедры технической защиты информации Национальной Академии Службы безопасности Украины.
Bogush Volodymyr, PhD in technical Sciences, associate professor of the Technical Information Security Department of National Academy of Security Service of Ukraine.