

УДК 004.056.5:378.1(045)

Бурячок Володимир Леонідович

доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID 0000-0002-4055-1494
v.buriachok@kubg.edu.ua

Богуш Володимир Михайлович

кандидат технічних наук, доцент, професор спеціальної кафедри
Національна академія Служби безпеки України, Київ, Україна
ORCID ID 0000-0002-2581-0988
bogush_vm@ukr.net

Борсуковський Юрій Володимирович

кандидат технічних наук, професор кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID 0000-0003-1973-2386
gmbyurii@gmail.com

Складанний Павло Миколайович

старший викладач кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Борсуковська Вікторія Юрївна

керівник проектів
ПАТ «Укрсоцбанк», департамент безпеки, Київ, Україна
ORCID ID 0000-0002-4929-6987
v.barsik@gmail.com

МОДЕЛЬ ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ УКРАЇНИ

Анотація. У статті проаналізовано найбільш критичні світові загрози в інформаційній сфері і, як результат, зроблено висновок про посилення інформаційної конфронтації та нагнітання напруженості у відносинах між країнами. Такий стан справ вимагає якісного нового підходу до підготовки ІТ фахівців, з орієнтуванням її передусім на практичну площину в сфері інформаційної і кібернетичної безпеки та з урахуванням найбільш актуальних умінь і навичок, які повинен отримати майбутній фахівець в галузі кібернетичної безпеки. Для вирішення цього завдання в статті визначено найбільш пріоритетні ключові напрямки підготовки таких фахівців. За результатами аналізу законодавства України в галузі інформаційної та кібербезпеки, а також типового навчального плану НАТО з кібербезпеки в статті запропоновано приклади моделей компетентностей з підготовки фахівців для національної системи кібербезпеки. З огляду на те, 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 і Національний банк України, у статті запропоновано узгоджені з покладеними на ці структури завданнями, моделі професійних компетентностей для підготовки співробітників / особового складу цих організацій. Як результат, запропоновані в статті моделі професійних компетентностей можуть бути покладені в основу розробки / вдосконалення освітніх програм та навчальних планів підготовки фахівців у сфері кібербезпеки насамперед на першому, бакалаврському рівні вищої освіти, а також стати основою для коригування відповідного стандарту, узгодженого у 2017 році національним агентством із забезпечення якості вищої освіти. Надалі це зможе сприяти створенню нових стандартів з кібербезпеки як на другому (магістерському), так і третьому (освітньо-науковому) рівнях.

Ключові слова: безпека; інформація; інфраструктура; інфосфера; кібербезпека; кіберзагроза; кібероборона; кіберпростір; компетентність; система.

1. ВСТУП

Постановка проблеми. Людству (за оцінками науковців [1]) понад 60 тисяч років. За цей час змінилося майже 1800 поколінь, але лише одному з них виявилась підвладна інформаційна глобалізація [1], виникненню якої у XVIII – XIX ст. сприяли:

по-перше, чотири світові індустріальні та одна інформаційна революції [2];

по-друге, винайдення двох простих, але дуже змістовних законів, сформульованих Гордоном Муром та Робертом Меткалфом [3].

Саме це, у свою чергу, обумовило появу і формування інформаційного та кібернетичного просторів, сприяло формуванню сучасного інформаційного суспільства і призвело до синтезу двох технологій – інформаційної та телекомунікаційної, але разом з цим питання щодо міждержавного паритету та взаємовідносин в інформаційному і кіберпросторах (на відміну від таких просторів, як наземний, морський, повітряний та космічний) залишило відкритими і такими, що й донині потребують свого розв'язку. Такий стан справ пояснюється передусім безпрецедентним впливом на сучасне суспільство та його інформаційний і кібернетичний простір низки цілеспрямованих інформаційних та кібероперацій, що стало останнім часом невід'ємною частиною внутрішньої і зовнішньої політики переважної більшості держав земної кулі, починає відігравати суттєву роль в їх економічному і соціальному розвитку та свідчить про їх вступ до якісно нової фази суспільних взаємовідносин – інформаційного та кіберпротистояння.

Разом із вибуховим зростанням обсягів даних, до яких отримали доступ пересічні громадяни, та їх переведенням в хмарну інфраструктуру, а також винайденням потужних комп'ютерів та вбудованих мікроконтролерів усе це спонукає країни світу не тільки до глобальної інтелектуалізації й отримання певних переваг, але й сприяє виникненню низки проблем, пов'язаних з безпекою, роблячи при цьому більш вразливими критично-важливі об'єкти інфраструктури цих країн до загроз антропогенно-техногенного характеру та природних катаклізмів. Вперше 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 найближчій перспективі відіграватимуть надзвичайно важливу роль у міжнародній геополітичній конкуренції. Черговим разом питання щодо боротьби із світовими кіберзагрозами стало темою для обговорення в рамках Давоського форуму «Створення спільного майбутнього в мінливому світі» у 2018 році. У ході форуму експертами було оприлюднено оцінку сучасного ландшафту глобальних загроз [4], що наведено на рис.1.

З іншої сторони є показовою оцінка компанії R-Visio, яка на основі аналізу прогнозів вендорів (компаній-поставщиків) щодо рішень з інформаційної безпеки (ІБ) сформувала власний ТОП-10 загроз в інформаційній сфері на поточний 2018 рік [5]. До таких загроз на думку представників компанії слід віднести:

- *використання машинного навчання і штучного інтелекту* – буде застосовуватись машинне навчання і штучний інтелект для автоматизованого пошуку вразливостей, підвищення точності атак, проведення більш витончених фішингових атак;
- *подальший розвиток вірусів-вимагачів* – програми-вимагачі залишаться

ключовою складовою ландшафту кіберзагроз в 2018 році, їх сімейство буде рости, а фокус хакерів зміститься на мобільні пристрої;

- *атаки на хмарну інфраструктуру і сховища* – очікуються витік даних із публічних хмарних сховищ, у результаті яких з'явиться доступ до персональних ключів, паролів, приватної інформації і навіть інтелектуальної власності;
- *експлуатацію уразливостей в пристроях класу інтернету речей (IoT)* – вразливості в галузі IoT будуть використовуватись все частіше, оскільки багато пристроїв виробляються без урахування правил безпеки і галузевих стандартів;

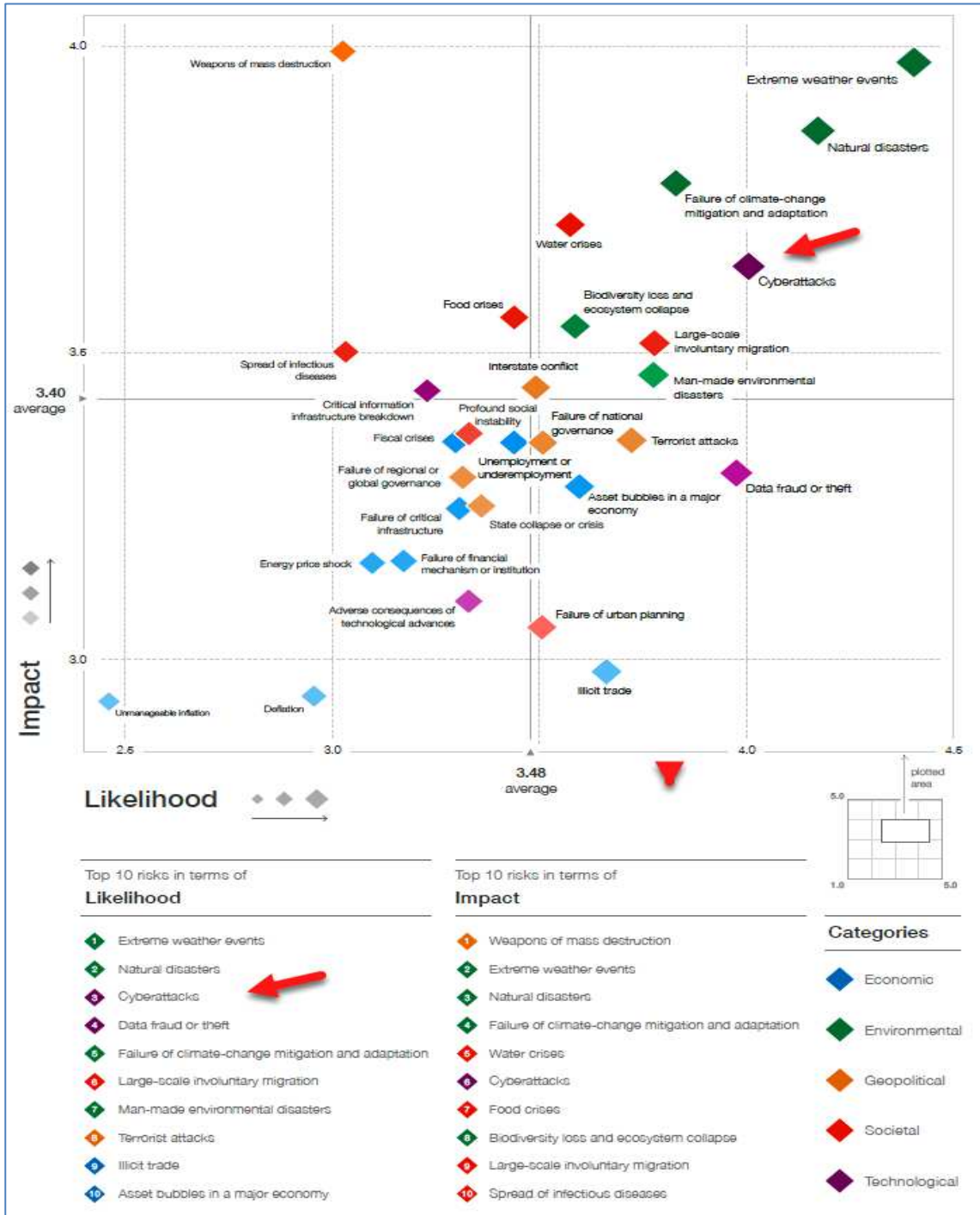


Рис. 1. Глобальний ландшафт загроз 2018 року

- *зломи засобів масової інформації і акаунтів в соціальних мережах для поширення неправдивої інформації* – вплив на котирування фондових бірж, маніпуляції громадською думкою, негативний вплив на репутацію, пропаганда через зламані канали і т.д.;
- *зростання атак на промислові підприємства* – набере обертів підготовка і реалізація складних кібератак на промислові об'єкти з використанням кібершпіонажу й експертних знань про АСУ ТП і специфіку галузей;
- *нашесть безфайлових і полегшених вірусів (ghost malware)* – ghost malware не записує на жорсткий диск файли і виконує всі свої дії в пам'яті, у момент перезавантаження системи вірус зникає, але збиток від нього вже системі завданий, виявити, відстежити і зупинити таку атаку досить важко;
- *атаки на мобільні додатки* – основною мішенню стануть Android і iOS платформи - збільшення частоти атак і вдосконалення технологій їх знешкодження призведе до виникнення більш складних АРТ-шкідників для мобільних платформ;

Враховуючи це, експерти, присутні на Всесвітньому економічному форумі, прийшли до такого висновку: світ нині вступив у той період свого розвитку, коли світова критична енергія сфокусована передусім на розпалювання розбрату. Підтвердженням такому є приклади масових випадків шахрайства даних та/або їх крадіжки, які призводять не тільки до значної економічної шкоди, але і провокують геополітичну напруженість та втрату довіри в Інтернеті, що автоматично може призводити до значної соціальної нестабільності з непрогнозованими наслідками [6]. Разом з тим, створення та поширення перспективних інформаційних систем і технологій сприяє появі нових форм кібератак, що піддають урядові та корпоративні ресурси загрозам, з якими вони не готові мати справу. Найбільш вживаними при цьому згідно статистики є DDoS-атаки, а найбільш небезпечними серед атак вважають АРТ-атаки. Узагальнену схему здійснення таких атак подано на рис. 2 [7], [8].

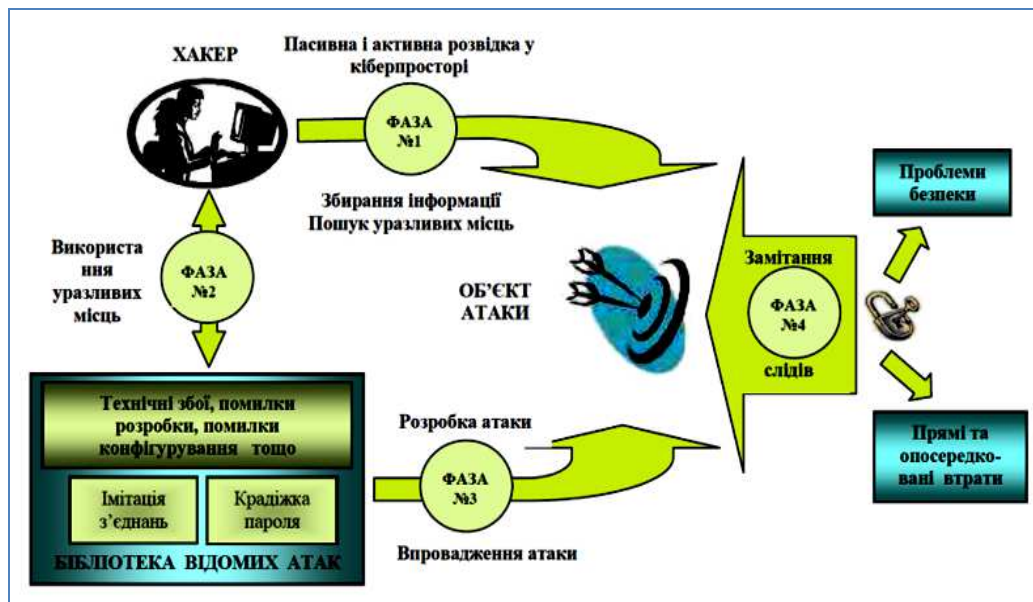


Рис .2. Узагальнена схема здійснення хакерської атаки

Усе це потребує нового підходу до підготовки відповідних фахівців, здатних у стислі терміни реагувати на кіберінциденти та протидіяти кіберзагрозам, проводити аудити станів інформаційної та кібербезпеки (ІКБ), створювати ефективні системи

управління ІКБ тощо [9]. Дослідженню означеної проблеми присвячені праці Даника Ю. Г. [10], Міночкина А. І. [11], Сисоєва В. [12], Супрунова Ю. М. [10] та інших. Проте в цих працях відсутній підхід до формування моделі компетентностей, яка може бути покладена в основу розробки освітніх програм та навчальних планів для якісної підготовки фахівців з кібербезпеки. Зважаючи на таке **метою даної роботи** є вироблення низки пропозицій щодо коригування загальної моделі компетентностей за погодженням у 2017 році Національним агентством із забезпечення якості вищої освіти стандартом [13], а також створення нових стандартів стосовно навчання методам превентивного забезпечення кібербезпеки на наступних освітньо-професійному та освітньо-науковому рівнях.

2. ТЕОРЕТИЧНІ ОСНОВИ 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» [14]. Найбільш актуальними вміннями та навичками у найближчому майбутньому, як вважає міжнародна спільнота [14], будуть:

- | | |
|---|-------------------------------------|
| 1) вміння вирішувати складні задачі; | 6) навички емоційного інтелекту; |
| 2) вміння критично мислити; | 7) вміння приймати рішення; |
| 3) вміння бути креативним; | 8) навички орієнтування на клієнта; |
| 4) вміння управляти людьми; | 9) вміння вести перемовини; |
| 5) навички до координації та взаємодії; | 10) навички когнітивної гнучкості. |

Разом із цим, як у процесі коригування моделі компетентностей на бакалаврському рівні, так й у ході створення нових стандартів з навчання методам превентивного забезпечення 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 віртуальних активів від загроз порушення конфіденційності, цілісності та доступності, але в деяких абстрактних рамках – у кіберпросторі (рис. 3) [15].



Рис. 3. Взаємозв'язок понять безпека, простори інформаційний та кібернетичний

Що стосується питання забезпечення кібербезпеки, то в якості пріоритету доцільно виділити координацію взаємодії між організаціями, що формують кіберпростір, але самостійні дії яких не забезпечують ефективний захист від

кіберзагроз. Очевидно, що прикладна галузь кібербезпеки (рис.4) є тісно інтегрованою з поняттями інформаційної безпеки (ІБ), безпекою застосувань, мережною безпекою, безпекою глобальних мереж, а також безпекою критичних інформаційних інфраструктур.



Рис. 4. Прикладна галузь інформаційної та кібербезпеки

При цьому: безпека застосувань визначається у відношенні до 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. Власне 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.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

На сьогоднішній день експерти визначають такі основні ключові напрямки, які повинні потрапити в сферу пріоритетної уваги під час підготовки фахівців із кібербезпеки [7], [8], [15]:

- аналіз поточних атак та сучасних вимог до ІТ-технологій;
- аутентифікація, шифрування і створення білих списків додатків;
- аналіз і зіставлення прийнятих рішень з існуючими методологіями і посібниками;
- підходи до застосування продуктів забезпечення ІКБ;
- проведення тестування на наявність уразливостей та перевірки на відповідність діючим стандартам безпеки;
- використання рекомендацій світової спільноти у створенні галузевих систем інформаційної безпеки.

Тут повною мірою можна використовувати рекомендації CIS [16], [17] для створення окремих навчальних профілів підготовки фахівців із захисту інформаційних

державних та корпоративних систем. Ці профілі повинні включати в себе підходи та методики щодо всебічних перевірок елементів IT-інфраструктури, конфігурацій, прав доступу, привілеїв, системних журналів, заходів і засобів реагування на інциденти та принципи ініціювання перевірок. У сьомій редакції керівництва CIS Controls [16], [17] дані елементи розподілені на три категорії, що враховують сучасний ландшафт кіберзагроз (табл. 1) – базові, фундаментальні та організаційні.

Таблиця 1

Категорії CIS

Базові категорії	Фундаментальні категорії	Організаційні категорії
<ul style="list-style-type: none"> – інвентаризація авторизованих і неавторизованих пристроїв; – інвентаризація авторизованого і неавторизованого програмного забезпечення; – засоби управління уразливостями; – використання адміністративних привілеїв; – захищені конфігурації для мобільних пристроїв, ноутбуків, робочих станцій і серверів; – обслуговування, моніторинг та аналіз журналів аудиту 	<ul style="list-style-type: none"> – захист електронної пошти та веб-браузера; – захист від шкідливих програм; – обмеження і контроль мережевих портів; – можливість відновлення даних; – захищені конфігурації для мережевих пристроїв (файрволи, роутери, комутатори); – захист периметра; – захист даних; – контроль доступу; – контроль доступу бездротових мереж; – контроль облікових записів 	<ul style="list-style-type: none"> – контроль рівня обізнаності персоналу; – контроль прикладного програмного забезпечення; – реагування на інциденти; – тестування на проникнення

Резюмуючи наведене вище, можна визначити, наприклад, відповідно до типового навчального плану з кібербезпеки [14], декілька основних класів моделі професійних компетентностей у сфері підготовки фахівців для національної системи 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 формування ландшафту кібербезпеки. Причому компетентності щодо основ ідентифікації ризиків і управління ними повинні бути головним спільним елементом, що пов'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 використання таких уразливостей при застосуванні різних схем проникнення в інформаційні системи та формуванні деструктивних векторів нападу. Розуміння характеру таких уразливостей – невід'ємний компонент ризику і принципів зниження його рівня.

Третій клас професійних компетентностей складають компетентності щодо розуміння принципів діяльності міжнародних організацій, формування політик та стандартів у сфері кібербезпеки. Вони полягають у змозі визначити роль організацій за міжнародними стандартами, розуміти ключові принципи національної політики у сфері кібербезпеки в контексті міжнародних стандартів і рекомендованого досвіду, порівнювати їх з різними прикладами національних принципів, а також оцінювати

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 ефективного управління кібербезпекою та рівнем національної готовності у сфері кібербезпеки в узгодженні з контекстом оцінок ризиків. Це можуть бути:

- компетентності щодо національних методів роботи, принципів дії та організації щодо кіберстійкості, планування послідовності дій в разі виникнення надзвичайних обставин і в процесі відновлення після кіберінцидентів, з метою нейтралізації дестабілізуючих чинників, що призвели до критичних ситуацій в інформаційному просторі;
- компетентності щодо національних методів управління кібербезпекою, що включають заходи забезпечення кібербезпеки, реагування на надзвичайні ситуації та мінімізацію ризиків;
- компетентності щодо інструментів, методів і процедур у сфері цифрової криміналістики з метою збору, аналізу та інтерпретації даних для встановлення атрибуції і спеціальних вимог для спецслужб;
- компетентності щодо контролю й оцінки безпеки на національному рівні, та оцінки готовності у сфері забезпечення національної кібербезпеки.

Результати навчання повинні бути такими:

- володіння методологічними і теоретичними основами 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 превентивного забезпечення кібернетичної безпеки;
- здатність застосовувати стандарти, процедури та додатки для забезпечення конфіденційності, цілісності та доступності інформації та ІС;
- здатність використовувати системи та інструменти, необхідні для мінімізації ризиків у кібернетичному просторі;
- здатність здійснювати організаційно-технічні заходи щодо виявлення загроз й інцидентів, реагування на інциденти та запобігання інцидентам, а також застосовувати методи відновлення інформаційних активів після інциденту;
- здатність здійснювати розроблення концепцій, технічних вимог, засобів проектування та реалізації системи управління кібербезпекою.

Наведені вимоги та твердження 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 (ДССЗІ) 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 відповідно до професійно-орієнтованих моделей компетентностей, які відповідають покладеним на них завданням (рис. 5) [7], [8]. При цьому, наприклад, для виконання завдань у системі забезпечення національної системи кібербезпеки ДССЗІ 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 до забезпечення створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту;
- здатність до здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків;
- здатність до забезпечення інформування про потенційні кіберзагрози та відповідні методи захисту від них;
- здатність до забезпечення управління аудитом інформаційної безпеки на об'єктах критичної інфраструктури, встановлення вимог 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 формування вимог щодо впровадження та використання системи безперервного навчання персоналу об'єктів критичної інформаційної інфраструктури методами та способам особистого кіберзахисту;
- здатність до виконання оперативних обов'язків в технологічних процесах функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

Для виконання завдань у системі національної системи забезпечення 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 до здійснення заходів 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 сформулювати й описати широке коло методологічних, наукових та технічних основ побудови кіберпростору;
- здатність сформулювати й описати процеси протидії у кіберпросторі; здатність аналізувати методи та засоби організації протидії у кіберпросторі провідних країн світу;
- здатність аналізувати тактику та стратегію спеціальних операцій у кіберпросторі;
- здатність аналізувати методи й засоби розвідувальної і контррозвідувальної діяльності у кіберпросторі;
- здатність організовувати розвідувальну та контррозвідувальну діяльність у кіберпросторі;
- здатність здійснювати контррозвідувальні та оперативно-розшукові заходи у кіберпросторі.

Відповідно до Конституції і законів України (зокрема Закону України «Про основні засади забезпечення кібербезпеки України» №2163-VII від 05.10.2017) основні суб'єкти національної системи кібербезпеки, а саме: 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 установленому порядку виконують такі основні завдання:



Рис. 5. Розподіл завдань між суб'єктами національної системи кібербезпеки

Для виконання завдань у системі національної системи кібербезпеки Міністерством оборони України і Генеральним штабом Збройних Сил України:

- здатність формулювати та 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;
- розробляти та впроваджувати 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 й 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 ризиків, стану кіберзахисту та результатів аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України.

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Підготовка фахівців для національної системи кібербезпеки може мати базову професійно-орієнтовану основу, яка, з одного боку, може ґрунтуватися на компетентностях та планово-прогнозованих результатах навчання, а з іншого боку, опиратися на стандарт вищої освіти та типовий навчальний план НАТО стосовно кібербезпеки. Очевидно, що така система підготовки фахівців для складових національної кібербезпеки, до яких відносяться 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, Національний банк України, повинна здійснюватися відповідно до розроблених та затверджених моделей професійних компетентностей, що дасть можливість підвищити ефективність підготовки фахівців відповідно до сформульованих та закладених у моделі завдань.

Запропоновану модель імплементовано в навчальні плани підготовки фахівців у сфері інформаційної та кібернетичної безпеки в Національній академії Служби безпеки України, Київському університеті імені Бориса Грінченка та Державному університеті телекомунікацій. У ході подальших досліджень буде здійснено обробку статистичних результатів, отриманих із зазначених навчальних закладів.

Наведені рекомендації можуть застосовуватися для всіх рівнів підготовки фахівців, включаючи перепідготовку та підвищення кваліфікації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] А. М. Прохоров, *Человек. Большой энциклопедический словарь*, 1993, 2-е изд., М., Большая российская энциклопедия, 1632 с.
- [2] М. Кастельс, *Информационная эпоха: экономика, общество и культура*, 2000, М., ГУ ВШЭ, 608 с.
- [3] В. П. Леонтьев, *Большая энциклопедия компьютера и Интернета*, 2005, М., ОЛМА-ПРЕСС Образование, 1104 с.
- [4] World Economic Forum, *Reports 2018* [Електронний ресурс]. Режим доступу: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf. Дата звернення: 24 Травня, 2018).
- [5] R-Vision, *Прогнозы по информационной безопасности на 2018 год* [Електронний ресурс]. Режим доступу: <https://rvision.pro/blog-posts/prognozy-po-informatsionnoj-bezopasnosti-na-2018-god/> Дата звернення: 24 травня 2018.
- [6] Euronews, *Давос 2018: совместный ответ глобальным угрозам* [Електронний ресурс]. Режим доступу: <http://ru.euronews.com/2018/01/24/davos-2018-what-are-humanitarian-organisations-bringing-to-the-world-economic>. Дата звернення: 24 травня 2018.
- [7] В. Л. Бурячок і В. М. Богуш, "Рекомендації щодо розробки та запровадження профілю навчання 'кібернетична безпека' в Україні", *Ukrainian Scientific Journal of Information Security*, 2014, №20, 2, сс. 126–131.
- [8] Ю. В. Борсуковський і В. Л. Бурячок, "Роль і місце вищих навчальних закладів у створенні системи інформаційної та кібернетичної безпеки України", *Сучасний захист інформації*, 2017, №1, сс. 34–40.
- [9] "Закон України Про основні засади забезпечення кібербезпеки України", 2017, ВВР, № 45, ст. 403 [Електронний ресурс]. Режим доступу: <http://zakon0.rada.gov.ua/laws/show/2163-19> Дата звернення: 24 травня 2018.
- [10] Ю. Г. Даник і Ю. М. Супрунов, "Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України", *Збірник наукових праць ЖВІ НАУ „Інформаційні системи“*, 2011, в"п. 5, сс. 5–22.
- [11] А. І. Міночкін, "Інформаційна боротьба: сучасний стан та досвід підготовки фахівців", *Оборонний вісник*, К., Центр воєнної політики та політики безпеки, 2011, №2, сс. 12–14.
- [12] В. Сисоев, "Аналіз рівня освіти та підготовки фахівців з управління ІТ та інформаційної безпеки в Україні", [Електронний ресурс]. Режим доступу: http://www.auditagency.com.ua/blog/ISACA_research_Education.pdf. Дата звернення: 24 травня 2018.
- [13] "Перший стандарт вищої освіти стосується кібербезпеки" [Електронний ресурс]. Режим доступу: <https://ligazakon.net/lawnews/doc/-nz173112-pershyy-standart-vyshchoyi-osvity-stosuyetsya-kiberbezpeky?type=ep>. Дата звернення: 24 травня 2018.
- [14] "Cybersecurity: A Generic Reference Curriculum (RC). Dear Partners/NATO Members, 4500-1 (OSEM PED)", Oct. 2016, 73 p.
- [15] "ISO/IEC 27032:2012. Information technology — Security techniques — Guidelines for cybersecurity", 50 p.
- [16] Center for Internet Security, *CIS Controls Version 7 — What's Old, What's New* [Електронний ресурс]. Режим доступу: <https://www.cisecurity.org/cis-controls-version-7-whats-old-whats-new/>. Дата звернення: 24 травня, 2018.
- [17] Center for Internet Security. *CIS Controls* [Електронний ресурс]. Режим доступу: <https://www.cisecurity.org/controls/>. Дата звернення: 24 травня, 2018.

Матеріал надійшов до редакції 16.05.2018р.

МОДЕЛЬ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В СФЕРЕ ІНФОРМАЦІОННОЇ І КІБЕРНЕТИЧЕСКОЇ БЕЗОПАСНОСТІ В УЧРЕЖДЕНИЯХ ВЫСШЕГО ОБРАЗОВАНИЯ УКРАИНЫ

Бурячок Владимир Леонидович

доктор технических наук, профессор, заведующий кафедрой информационной и кибернетической безопасности

Киевский университет имени Бориса Гринченко, Киев, Украина

ORCID ID 0000-0002-4055-1494

v.buriachok@kubg.edu.ua

Богущ Володимир Михайлович

кандидат технических наук, доцент, профессор специальной кафедры
Национальная академия Службы безопасности Украины, Киев, Украина
ORCID ID 0000-0002-2581-0988
bogush_vm@ukr.net

Борсуковский Юрий Владимирович

кандидат технических наук, профессор кафедры информационной и кибернетической безопасности
Киевский университет имени Бориса Гринченко, Киев, Украина
ORCID ID 0000-0003-1973-2386
gmbuyurii@gmail.com

Складанный Павел Николаевич

старший преподаватель кафедры информационной и кибернетической безопасности
Киевский университет имени Бориса Гринченко, Киев, Украина
ORCID ID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Борсуковская Виктория Юрьевна

руководитель проектов
ПАО «Укрсоцбанк», департамент безопасности, Киев, Украина
ORCID ID 0000-0002-4929-6987
v.barsik@gmail.com

Аннотация. В статье проанализированы наиболее критичные международные угрозы в информационной сфере и, как результат, сделан вывод об усиливающейся информационной конфронтации и нагнетании напряженности в отношениях между странами. Такое состояние дел требует качественного нового подхода к подготовке ИТ специалистов, с ориентированием ее прежде всего на практическую плоскость в сфере информационной и кибернетической безопасности, с учетом наиболее актуальных умений и навыков, которые должен получить будущий специалист в области кибербезопасности. Для решения этой задачи в статье определены наиболее приоритетные ключевые направления подготовки таких специалистов. По результатам анализа законодательства Украины в области информационной и кибербезопасности, а также типового учебного плана НАТО по кибербезопасности в статье предложены примеры моделей компетентностей по подготовке специалистов для национальной системы кибербезопасности. Учитывая то, что основными субъектами национальной системы кибербезопасности, в соответствии с Конституцией и законами Украины, является Государственная служба специальной связи и защиты информации Украины, Национальная полиция Украины, Служба безопасности Украины, Министерство обороны Украины и Генеральный штаб Вооруженных Сил Украины, разведывательные органы и Национальный банк Украины, в статье предложены согласованные с возложенными на эти структуры задачами, модели профессиональных компетентностей для подготовки сотрудников /личного состава данных организаций. Как результат, предложенные в статье модели профессиональных компетентностей могут быть положены в основу разработки / усовершенствования образовательных программ и учебных планов подготовки специалистов в области кибербезопасности прежде всего на первом, бакалаврском уровне высшего образования, а также стать основой для корректировки соответствующего стандарта, согласованного в 2017 году Национальным агентством по обеспечению качества высшего образования. В дальнейшем это сможет способствовать созданию новых стандартов по кибербезопасности как на втором (магистерском), так и третьем (образовательно-научном) уровнях.

Ключевие слова: безопасность; информация; инфраструктура; инфосфера; кибербезопасность; киберугроза; кибероборона; киберпространство; компетентность; система.

TRAINING MODEL FOR PROFESSIONALS IN THE FIELD OF INFORMATION AND CYBER SECURITY IN THE HIGHER EDUCATIONAL INSTITUTIONS OF UKRAINE

Volodymyr L. Buriachok

Doctor of Technical Sciences, Professor, Head of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID 0000-0002-4055-1494
v.buriachok@kubg.edu.ua

Volodymyr M. Bogush

PhD in technical Sciences, Associate Professor, Professor of the Special Chair
National Academy of Security Service of Ukraine, Kiev, Ukraine
ORCID ID 0000-0002-2581-0988
bogush_vm@ukr.net

Yurii V. Borsukovskii

PhD in technical Sciences, Professor of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID 0000-0003-1973-2386
gmbyurii@gmail.com

Pavlo M. Skladannyi

Senior Lecturer of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Victoria Yu. Borsukovska

PJSC "Ukrsotsbank", Security Department, Kyiv, Ukraine
ORCID ID 0000-0002-4929-6987
v.barsik@gmail.com

Abstract. The most critical global security threats in the information sphere are analyzed in the article, and, as a result, it was made a conclusion about the increasing of information confrontation and infiltration of tension in relations between countries. This situation requires a new qualitative approach to IT specialists' training, focusing their attention primarily on the practical plane in the field of information and cyber security, and taking into account the most relevant expertise that a future specialist should receive in the field of cyber security. To solve this problem, the most important priority areas for the training of such specialists are identified in the article. According to the results of the analysis of Ukrainian legislation in the field of information and cyber security, as well as the typical cyber security plan of the NATO, examples of models of training competencies for the national cyber security system are proposed in the article. Considering that the main subjects of the national system of cyber security in accordance with the Constitution and laws of Ukraine are the State Service for Special Communications and Information Protection of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence agencies and the National Bank of Ukraine, the models of professional competences of the employees/personnel of these organizations training, agreed with the tasks entrusted to these structures, are proposed in the article. As a result, the proposed models of professional competences may be the basis for the development / improvement of educational programs and curricula for training specialists in the field of cyber security, especially at the first, Bachelor's level of higher education, and may become the basis for adjusting the relevant standard agreed in 2017 by the national Agency for Quality Assurance in Higher Education. In the future, the creation of new standards for cyber-security, both in the second (master's) and in the third (educational-scientific) levels will be promoted.

Keywords: security; information; infrastructure; infosphere; cyber security; cyber threat; cyber defense; cyber space; competence; system.

REFERENCES (TRANSLATED AND TRANSLITERATED)

- [1] A. M. Prokhorov, *Human. The great encyclopedic dictionary*, 1993, 2nd ed., M., Bol'shaya rossiiskaya entsiklopediya, 1632 p. (in Russian).
- [2] M. Kastel's, *Information age: economy, society and culture*, 2000, M., GU VShE, 608 p. (in Russian).
- [3] V. P. Leont'ev, *Great encyclopedia of computer and Internet*, 2005, M., OLMA-PRESS Obrazovanie, 1104 p. (in Russian).
- [4] World Economic Forum, *Reports 2018* [Online]. Available: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf. Accessed on: May 24, 2018.
- [5] R-Vision, *Information security forecasts for 2018*. [Online]. Available: <https://rvision.pro/blog-posts/prognozy-po-informatsionnoj-bezopasnosti-na-2018-god/>. Accessed on: May 24, 2018. (in Russian).
- [6] Euronews, *Davos 2018: a joint response to global threats*. [Online]. Available: <http://ru.euronews.com/2018/01/24/davos-2018-what-are-humanitarian-organisations-bringing-to-the-world-economic>. Accessed on: May 24, 2018. (in Russian).
- [7] V. L. Buryachok and V. M. Bohush, Recommendations for developing and implementing a training profile, cybernetic security in Ukraine,” *Ukrainian Scientific Journal of Information Security*, 2014, no. 20, 2, pp. 126–131. (in Ukrainian).
- [8] Yu. V. Borsukov's'kyi and V. L. Buryachok, The role and place of higher educational establishments in the creation of a system of information and cybernetic security of Ukraine,” *Suchasnyy zakhyst informatsiyi*, 2017, no. 1, pp. 34–40. (in Ukrainian).
- [9] The law of Ukraine on the basic principles for the cybersecurity of Ukraine,” 2017, VVR, no. 45, art. 403 [Online]. Available: <http://zakon0.rada.gov.ua/laws/show/2163-19>. Accessed on: May 24, 2018. (in Ukrainian).
- [10] Yu. H. Danyk and Yu. M. Suprunov, Some approaches to the formation of a system of training for the system of cybernetic security of Ukraine,” *Zbirnyk naukovykh prats' ZhVI NAU “Informatsiyini systemy,”* 2011, no. 5, pp. 5–22. (in Ukrainian).
- [11] A. I. Minochkin, Information struggle: current state and experience of training specialists, *Oboronnyy visnyk*, K., Tsentr voyennoyi polityky ta polityky bezpeky, 2011, no. 2, pp. 12–14. (in Ukrainian).
- [12] V. Sysoyev, *Analysis of the level of education and training of specialists in the management of IT and information security in Ukraine* [Online]. Available: http://www.auditagency.com.ua/blog/ISACA_research_Education.pdf. Accessed on: May 24, 2018. (in Ukrainian).
- [13] The first standard of higher education concerns cybersecurity. [Online]. Available: <https://ligazakon.net/lawnews/doc/-nz173112-pershyy-standart-vyshchoyi-osvity-stosuyetsya-kiberbezpeky?type=ep>. Accessed on: May 24, 2018. (in Ukrainian).
- [14] “Cybersecurity: A Generic Reference Curriculum (RC). Dear Partners/NATO Members, 4500-1 (OSEM PED),” Oct. 2016, 73 p. (in English)
- [15] “ISO/IEC 27032:2012. Information technology — Security techniques — Guidelines for cybersecurity,” 50 p. (in English)
- [16] Center for Internet Security, *CIS Controls Version 7 — What's Old, What's New* [Online]. Available: <https://www.cisecurity.org/cis-controls-version-7-whats-old-whats-new/>. Accessed on: May 24, 2018. (in English)
- [17] Center for Internet Security. *CIS Controls* [Online]. Available: <https://www.cisecurity.org/controls/>. Accessed on: May 24, 2018. (in English)

