УДК 343.98:378(038)

Віталій Борисович ЧЕРЕДНИЧЕНКО,
старший викладач кафедри соціально-економічних дисциплін Сумської філії Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-4733-453X;
Ігор Анатолійович КУЛИК,
кандидат технічних наук, доцент,
доцент кафедри електроніки та комп'ютерної техніки Сумського державного університету

ВИЗНАЧЕННЯ НАПРЯМКІВ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ДЛЯ ПОЛІЦІЇ УКРАЇНИ

В останні роки спостерігається значне зростання кіберзлочинності у багатьох країнах світу. На об'єкти енергосистем, авіаційного та залізничного транспорту, фінансової системи, сервери телевізійних каналів, державних установ з Інтернету здійснюється все більше атак. Введені у обіг терміни «кіберзброя», «кібервійна» та «кібертероризм» досить точно відображають суть цих нових загроз.

Забезпечення кібербезпеки в органах влади, на промислових об'єктах, у військовій сфері, захист баз даних МВС, виявлення та розслідування кіберзло-чинів – вимагають від фахівців з кібербезпеки засвоєння *предметно – спеціальних* компетентностей по двох напрямках. Перший – це загально – професійний набір компетентностей з напрямку кібербезпеки. Другий – це галузево – професійний набір знань та навичок відповідно до сфери практичної діяльності. Розглянемо підходи до формування загальних та галузевих професійних компетентностей у навчальних програмах для співробітників Національної поліції по спеціальності 125 «Кібербезпека».

Указом Президента України від 15 березня 2016 року № 96/2016 затверджена «Стратегія кібербезпеки України». Указ вимагає невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України. У ньому визначено основні напрямки забезпечення кібербезпеки: ефективна боротьба із кіберзагрозами, кібершпигунством, кібертероризмом та кіберзлочинністю; забезпечення кіберзахисту державних електронних інформаційних ресурсів, критичної інформаційної інфраструктури та життєво важливих інтересів людини, суспільства та держави в кіберпросторі. Указ визначає, що основу національної системи кібербезпеки становлять: Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи. Цим Указом на Національну поліцію України покладено забезпечення захисту людини, суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення та розкриття кіберзлочинів [1].

Джерелом, яке формує набір загально – професійних компетентностей для фахівців кібербезпеки, є розроблений Міністерством освіти і науки України у 2016 р. «Стандарт вищої освіти України: галузь знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека». Розділ Стандарту «Фахові результати навчання» містить 41 найменування, які по суті формулюють зміст дисциплін для усіх професіоналів даної спеціальності [2]. Стандарт є обов'язковим при підготовці усіх фахівців з кібербезпеки, як цивільних, так і міліарних. Але ВНЗ силових відомств (МО, МВС, СБУ, розвідка) повинні дати своїм випускникам додатково знання та навички у сферах правоохоронної, оперативно-розшукової, військової, розвідувальної та іншої діяльності.

Джерелом набору галузево – професійних компетентностей для системи МВС є Положення про Департамент Кіберполіції (ДКП) Національної поліції України, затверджене наказом № 85 від 10.11.2015 р. Цим Положенням визначено основні завдання Департаменту Кіберполіції:

– попередження, виявлення та припинення кримінальних правопорушень у сфері кіберзлочинності;

– збір та узагальнення інформації стосовно об'єктів, що становлять оперативний інтерес, у тому числі у сферах телекомунікації, Інтернет послуг, банківських установ і платіжних систем;

– оперативно-розшукові заходи щодо викриття причин і умов, які призводять до кримінальних правопорушень у сфері кіберзлочинності;

– формування інформаційних масивів даних, автоматизованих інформаційних систем відповідно до потреб службової діяльності ДПК;

– виконання доручень слідчого, прокурора щодо проведення слідчих, розшукових дій (включаючи негласні дії) у кримінальних провадженнях;

– функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами, при переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі;

– функціонування локальних експертних лабораторій ДКП та мобільних груп швидкого реагування, призначених для виїзду до місць вчинення кримінальних правопорушень та з метою зняття даних з носіїв інформації;

– налагодження взаємодії з органами державної влади, іншими правоохоронними органами, партнерські відносини з приватним сектором та правоохоронними органами іноземних держав, міжнародними установами та організаціями у сфері протидії кіберзлочинності [3].

Аналізуючи усі завдання Кіберполіції, їх можна розділити на дві групи:

– оперативно – розшукові заходи, виявлення та розкриття злочинів, виконання доручень слідчого, негласні дії, цілодобовий виїзд груп швидкого реагування, переслідування злочинців, припинення злочинів;

– збір інформації про об'єкти, збирання доказів в електронній формі, аналітична робота, експертна лабораторія, взаємодія з населенням, державними органами, приватним сектором, правоохоронними органами (у т. ч. іноземними).

Для виконання цих завдань доцільно готувати офіцерів поліції за спеціальністю «Кібербезпека» по двох спеціалізаціях, які можна умовно назвати як оперативно-розшукова та аналітично-експертна. По цих спеціалізаціях повинен викладатись один спільний пакет базових дисциплін та два набори відповідних предметів та тренінгів.

Джерелом набору *предметно-спеціальних* компетентностей (subject specific competences) для фахівців кібербезпеки (cybersecurity specialist) є міжна-родний стандарт викладання комп'ютерних наук Computer Science Curricula, редакція CS2013 (ACM / IEEE-CS) [4]. Цей документ вважається міжнародним еталоном для викладання комп'ютерних наук. Так, усі університети США, що випускають фахівців з комп'ютерних наук, повинні підтвердити відповідність своїх програм державному стандарту, заснованому на Computing Curricula. По змісту «Computer Science Curricula 2013» – це детальний (180 сторінок) перелік компетентностей для підготовки бакалаврів комп'ютерних наук.

У літературі вказується, що розроблені протягом останніх років галузеві стандарти вищої освіти МОН України із напрямів підготовки ІТ-фахівців за освітньо-кваліфікаційним рівнем «бакалавр» гармонізовані з міжнародними документами Computing Curricula 2001–2005 та навчальними програмами провідних університетів світу. Бажано самім університетам перевірити відпо-відність своїх навчальних планів змісту «Computer Science Curricula 2013».

Вищим навчальним закладам доцільно формувати такі набори компетентностей спеціальності «Кібербезпека», які відповідають державним та галузевим завданням по забезпеченню кібербезпеки держави, суспільства та особи, особливо під час гібридної війни з сусідньою країною.

Список бібліографічних посилань

1. Стратегія кібербезпеки України : указ Президента України від 15.03.2016 № 96/2016. *Офіційний вісник Президента України.* 2016. № 10. С. 39.

2. Стандарт вищої освіти України. Галузь знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека». URL: www.mon.gov.ua/content/Новини/2016/125-kiberbezpeka.doc (дата звернення: 02.11.2017).

3. Департамент кіберполіції Національної поліції // Національна поліція : тимчас. веб-сайт. URL: https://www.npu.gov.ua/uk/publish/article/1816252 (дата звернення: 02.11.2017).

4. Computer Science Curricula 2013. URL: https://sigai.-acm.org/static/pdf/CS2013 -EAAI2011panel-RequestForFeedback.pdf (дата звернення: 02.11.2017).

Одержано 03.11.2017