Деякі методологістичні аспекти підготовки кадрів для підрозділів кіберполіції в Україні

Світличний Віталій Анатолійович,

доцент кафедри кібербезпеки Харківського національного університету внутрішніх справ, кандидат технічних наук

На теперішній час складно переоцінити актуальність підготовки фахівців кібербезпеки, особливо під час російської агресії, коли гостро відчувається потреба в таких спеціалістах, тому що

кібербезпека – це одне з пріоритетних завдань держави, що визначено в основних нормативно-правових актах України.

Проблематика підготовки національних кадрів у сфері кіберебезпеки, міжнародний досвід організації навчального процесу, досягнення й пропозиції у сфері боротьбі з кіберзлочинністю досить часто обговорюється фахівцями в інформаційній сфері в монографіях, наукових статтях, тезах доповідей на наукових конференціях, семінарах, круглих столах і в засобах масової інформації. Багато аспектів підготовки фахівців кібербезпеки вивчали К. Бєляков, С. Битко, В. Бутузов, А. Волеводз, В. Голубєв, Д. Дубов, С. Кльоцкін, В. Мілашев, М. Литвинов, В. Мохор, Е. Рижков, В. Хахановський, Т. Тропіна, О.Орлов, Є. Тітуніна. Але наразі недостатньо ґрунтовних досліджень з проблем підготовки фахівців з протидії злочинам у сфері кібербезпеки.

Головними напрямами практичної діяльності фахівця з кібербезпеки є: протидія правопорушенням, що вчиняються з використанням високих інформаційних технологій; підвищення ефективності правоохоронної діяльності Національної поліції України за допомогою використання сучасних засобів управління; впровадження в діяльність поліції комп'ютерних систем обробки та аналізу інформації, сучасних інформаційних технологій та методик використання технічних засобів.

Міжнародний досвід свідчить, що комп'ютерні злочини мають розслідуватись лише тими підрозділами або співробітниками поліції, які мають спеціальні навички для ведення таких справ та пройшли відповідну підготовку. Тому що, робота з комп'ютерним обладнанням вимагає спеціальних знань і умінь.

Підготовкою фахівців з кібербезпеки займаються багато ВНЗ, в тому числі Харківський національний університет внутрішніх справ (ХНУВС), який здійснює підготовку фахівців з вищою освітою для підрозділів Національної поліції України, що займаються протидією кіберзлочинності, злочинам у сфері торгівлі людьми та моральності, у міжнародній сфері та транснаціональній злочинності. Готовність випускників ХНУВС до практичної діяльності на рівні професійної майстерності

визначається низкою кваліфікаційних та професійних вимог. У порівнянні з навичками уміння в напрямку кібербезпеки мають велику змінність, носять усвідомлений характер виконання дій з переходом у наукову творчість. Зміна вимог до характеру умінь є відповіддю на зростання наукової інформації, швидку заміну старих знань новими. У цих умовах особливого значення набуває оволодіння людиною не стільки комп'ютерною технікою з відповіднім програмним забезпеченням, скільки оперативною методикою виконання практичних завдань. Якщо такий підхід важливий у навчанні курсантів інших спеціальностей, то при підготовці фахівців з кібербезпеки він є цілком необхідним. Адже фахівцям з кібербезпеки частіше, ніж іншим поліцейським доводиться оновлювати свої знання, переглядати методи роботи, опановувати нові уміння. Це складний процес, що включає інтелектуальний, емоційний і вольовий прояв особистості.

На нашу думку, з метою більш якісної підготовки фахівців з кібербезпеки у ХНУВС потрібно враховувати академічні та професійні вимоги до спеціалістів в галузі програмування, комп'ютерних наук та інформаційно-комунікаційних технологій, а також у супутніх галузях. Тому курсантів потрібно навчити нестандартно мислити, добре володіти іноземною мовою, щоб спілкуватися зі своїми колегами з інших країн для ознайомлення з зарубіжним досвідом в галузі боротьби з кіберзлочинністю. При цьому значну увагу потрібно надавати вивченню та практичному застосуванню:

- технологій кібербезпеки при користуванні та розробці систем аналітичних досліджень;
- керування базами даних та знань;
- мережевих додатків та Internet-сервісів;
- протоколів передачі та шифрування даних.

Крім того потрібно ознайомлювати курсантів та студентів з методиками сертифікації, експертизи та проведення спеціальних досліджень (в тому числі з використанням паралельних та квантових обчислювальних середовищ) засобів і систем кібернетичного захисту інформаційних ресурсів.

Для вирішення вищевказаних питань на нашу думку потрібно створити у ХНУВС (на базі існуючої кафедри кібербезпеки) кафедру розкриття і розслідування кіберзлочинів. Основними напрямами науково-педагогічної діяльності кафедри буде:

- розробка та застосування методик розслідування кіберзлочинів;
- застосування інформаційно-аналітичної роботи в оперативно-розшуковій діяльності поліції;
- використання методик проведення експертиз під час розслідування кіберзлочинів;
- використання сучасних інформаційних технологій в оперативно-розшуковій, слідчий діяльності при розслідувані злочинів у сфері торгівлі людьми та моральності, у міжнародній сфері та транснаціональній злочинності.