

УДК 378.600.405.653

В. В. Марков**ОСНОВНІ ПРИНЦИПИ ПІДГОТОВКИ ФАХІВЦІВ
У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ**

На прикладі досвіду функціонування моделі професійно-орієнтованого навчання, впровадженої на факультеті підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ, охарактеризовано основні організаційні та педагогічні принципи підготовки фахівців у сфері протидії кіберзлочинності, надано рекомендації щодо її подальшого сталого розвитку та вдосконалення.

Ключові слова: кіберзлочинність, протидія кіберзлочинності, принципи професійної підготовки, випереджальне навчання, навчально-тренувальний центр боротьби з кіберзлочинністю та моніторингу кіберпростору, модель професійно-орієнтованого навчання.

Постановка проблеми. Потрібно визнати, що сьогодні Україна приголомшена суворими викликами: війна, економічна криза, злочинність (особливо її корупційна складова). Якщо взяти ці фактори в комбінації, то стає зрозуміло, що вони дійсно дуже перевантажують суспільство та уряд з його першочерговими потребами та обов'язками. Однак якщо поглянути на це як на виклики, на те, що треба подолати, то це першочергові мобілізуючі завдання для народу та його країни. Уряд, якому нічого запропонувати, в тому числі у боротьбі зі знесилюючими чинниками наявної ситуації, не буде сприйнятий і не зможе виконати поставлених перед ним нагальних поточних завдань. Ось чому зараз дуже важливо говорити про реальні досягнення в цій царині публічно, зокрема потрібно постійно інформувати громадськість щодо результатів підготовки фахівців, здатних вдало вирішувати проблеми подальшого розвитку суспільства. Слід навчитися доносити цю інформацію до зацікавлених інституцій, включаючи міжнародні, маючи на увазі важливість підтримки інноваційних рішень і перших ефективних кроків з боку великої кількості людей. Тільки тоді зусилля, в тому числі у сфері професійної підготовки фахівців з протидії кіберзлочинності, будуть гідні публічної підтримки та обов'язково її отримають. Для успіху потрібно регулярно повідомляти про хід проведення підготовки, про зміст тих змін, що відбуваються в ній. Без цього процес реформування існуючої моделі навчання буде постійно наштовхуватися на прикрі перешкоди.

Перший крок потрібно робити (і це логічно) у сфері мотивування майбутнього фахівця. Він уже успішно зроблений у Харківському національному університеті внутрішніх справ у сфері набору курсантів до колективу навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору. Курсантам запропоновано

© Марков В. В., 2015

регулярне вирішення практичних фахових завдань з можливістю цілодобового підвищення умінь і навичок у роботі з новітніми інформаційними технологіями з використанням реально існуючого технічного обладнання (банкомату, засобів нагляді і зняття інформації тощо). Це приваблює достатню кількість зацікавлених осіб не лише з навчальних груп факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми, а й з інших університетських підрозділів (факультету підготовки фахівців для підрозділів слідства, інституту кримінальної міліції тощо).

Стан дослідження. Актуальні проблеми професійної підготовки особистості, зокрема правоохоронців, аналізувалися багатьма фахівцями в галузі правознавства, педагогічних, психологічних та інших наукових галузей. Цьому предмету дослідження приділяли особливу увагу такі вчені, як О. М. Бандурка [1; 2], М. Ф. Головатий [3], В. Б. Захожай [4], В. А. Лапшина [5], П. Мирошніченко [6]. Ними, зокрема, були розглянуті питання впровадження активних форм навчання, інновацій у системі сучасної освіти, професіоналізму, а також професійної деформації правоохоронців.

Метою цієї статті є висвітлення основних принципів підготовки фахівців у сфері протидії кіберзлочинності з урахуванням новітніх тенденцій, що спостерігаються останнім часом в організації не лише поточних педагогічних процесів у відомчому виші, а й у галузі професійної правоохоронної діяльності.

Організація підготовки фахівців у сфері протидії кіберзлочинності (загальна характеристика) уже ставала предметом нашого дослідження, де вказувалося на функціонування у складі Харківського національного університету внутрішніх справ (далі – ХНУВС) факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми. Зазначалося, що на сьогодні факультет є єдиним в Україні навчальним підрозділом, спеціально створеним для підготовки фахівців з протидії кіберзлочинності для системи МВС України [7, с. 6–7].

Основні загальнопедагогічні та організаційні принципи підготовки фахівців у сфері протидії кіберзлочинності. Відомо, що принципами називають головні, вихідні положення теорії, вчення, науки, практичної діяльності, а також справедливої оцінки її результатів. Зазвичай, як у мисленні, так і в дійсності принципами пов'язують між собою певні сукупності фактів або явищ, що мають відношення одним до одного. Отже, це такі основоположні норми та правила, якими людини (тим більше спеціалісту в певній галузі) потрібно керуватися у професійній діяльності й від яких не повинно бути відступів. При цьому принципи служать основою кожного виду діяльності настільки, що в іншому випадку її результати можуть виявитися прямо протилежними очікуваним. З часом ті чи інші принципи стають переконаннями людини, її головними поглядами на життя і професію. Цим і продиктоване їх базове значення у справі

підготовки фахівців, зокрема у сфері протидії кіберзлочинності, у вищих навчальних закладах системи МВС України. Пошуком і формулюванням відповідних принципів як основи для всієї наступної практичної діяльності починається навчальний процес у кожному виді професійної підготовки. Підготовка фахівців у сфері протидії кіберзлочинності не є винятком.

На нашу думку, основні принципи професійної підготовки фахівців у названій сфері слід розділити на дві групи – загальнопедагогічні та організаційні. Під загальнопедагогічними принципами зазвичай розуміють достатньо традиційні підходи, що доволі широко застосовуються в навчально-тренувальній діяльності в розвинених країнах світу: доступність, комплексність, методичність і систематичність. Разом з тим вважаємо, що результативність та ефективність їх реалізації безпосередньо залежить саме від тієї послідовності, в якій ми їх перерахували та від сполучення з тими організаційними інноваційними підходами, що впроваджені нами в навчальний процес професійної підготовки майбутніх фахівців у сфері протидії кіберзлочинності. Отже, до першої групи основних принципів професійної підготовки висококваліфікованих фахівців у сфері протидії кіберзлочинності ми відносимо:

1. *Доступність.* Під доступністю розуміють поступовий рух від простого до більш складного компонента навчальної діяльності. Саме такий підхід до навчання надає курсантам можливість засвоїти навчальний матеріал взагалі. Слід зазначити, що принцип доступності не виключає, а навпаки, передбачає визначальну придатність суб'єкта до вирішення поставлених ним самим (або іншими) навчальних, а також інших видів завдань, наприклад, робочих і пізнавальних. Поступовість у нарошуванні кількості та складності завдань, що пропонується вирішити, корелюється з наявністю кадрового та мінімально необхідного матеріального забезпечення навчання (кваліфікації викладацького складу, відповідного обладнання тощо). Ретельна увага до цього, поряд зі сталою мотивацією курсантів до фахової професійної підготовки, зазвичай гарантує задовільне вирішення навчальних завдань.

2. *Комплексність.* Під нею ми розуміємо наявність багатьох компонентів у процесі професійної підготовки, що ведуть до формування та подальшого вдосконалення відповідних професійних умінь і навичок, а також застосування різноманітних засобів вирішення навчальних завдань.

3. *Методичність.* Маються на увазі послідовність, цілеспрямованість діяльності щодо організації вирішення навчальних завдань курсантами, відмежованість застосованих методик і способів від так званих відволікаючих факторів, що можуть відвести від правильних рішень поставлених проблем. Методичність засвоєння курсантами умінь і навичок протидії кіберзлочинності досягається за рахунок постійної участі в моніторингу кіберпростору на предмет виявлення

протиправного контенту в мережі Інтернет. Такий моніторинг здійснюється цілеспрямовано, за завданням і під керівництвом підрозділів МВС щодо протидії кіберзлочинності, а також міжнародними організаціями, які діють в цій сфері, на базі відповідних угод ХНУВС.

4. *Систематичність*. Під цим принципом ми розуміємо цілісність підходів до навчальної діяльності та циклічність відновлення повторення тих чи інших її видів з метою відпрацювання відповідних професійних умінь і навичок, методик вирішення поставлених проблем. Крім того, курсанти повинні знати про важливе значення регулярності роботи фахівця для досягнення високих результатів (згідно з відомим висловом: «Найбільш ефективна лише чітко спрямована діяльність, що здійснюється без великих перерв»). Практичною спрямованістю та систематичністю взагалі визначається результативність фахової професійної підготовки. У свою чергу, систематичність фахової професійної підготовки полягає в залученні курсантів до вирішення професійних робочих завдань у взаємодії з професійними фахівцями у сфері протидії кіберзлочинності на постійній основі, тобто у безпосередній участі в процесі протидії кіберзлочинності. Підкреслимо, що досягнення головної навчальної мети – підготовки висококваліфікованого фахівця, здатного з перших днів майбутньої служби в системі підрозділів боротьби з кіберзлочинністю виконувати поставлені завдання, – залежить від цілеспрямованої взаємодії факультету з відповідними центральним і територіальними підрозділами МВС України щодо протидії кіберзлочинності, а також координацією навчальної роботи з відповідними зусиллями міжнародних організацій, задіяних у цій сфері.

Щодо другої групи принципів – організаційних, запроваджених на факультеті з самого початку його заснування, – то їх сутність полягає у проблематизації, поетапності, професійній зорієнтованості навчання та взаємодії тієї чи іншої навчальної структури (у нашому випадку факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми) з відповідними практичними підрозділами системи МВС.

1. *Проблематизація*. Вимогу шукати і своєчасно знаходити відповіді на проблемні питання професійно-службової діяльності (особливо суто методологічного характеру: як? в який спосіб? яким чином?) ми вважаємо одним із найважливіших принципів професійної підготовки майбутніх фахівців у сфері боротьби з кіберзлочинністю не випадково. Організації навчальних проблемних ситуацій у процесі професійної підготовки фахівців у сфері протидії кіберзлочинності ми надаємо особливе значення тому, що з проблемами (тобто завданнями, які не мають очевидного рішення) фахівець з боротьби з кіберзлочинами стикається постійно. Це вимагає необхідності оволодіння вміннями дослідницької діяльності ще на етапі навчання. Саме тому вже з перших навчальних семестрів курсанти факультету

залучаються до участі в наукових гуртках кафедр, підготовки наукових повідомлень, доповідей на науково-практичних конференціях і кафедральних семінарах.

2. *Поетапність*. До принципів підготовки професійних фахівців у сфері протидії кіберзлочинності ми відносимо також поетапність протікання освітніх процесів, у вивченні та засвоєнні навчальної програми. На нашу думку, формування особистості кожного професійного фахівця повинно проходити чотири головні етапи: 1) загальна підготовка (універсальний етап); 2) спеціальна підготовка (етап спеціалізації); 3) професійна підготовка (етап професіоналізації); 4) подальше кваліфікаційне зростання. Факультет ставить завдання реалізації в навчальному процесі всіх означених етапів на максимально високому рівні ефективності. На наш погляд, послідовне їх втілення гарантує вихід на достатньо високий рівень оволодіння тими професійно значущими знаннями, уміннями та навичками, які необхідні фахівцям у сфері протидії кіберзлочинності.

На етапі спеціалізації відбувається набуття спеціальних знань (початок фахової підготовки), на етапі професіоналізації – перехід до безпосереднього оволодіння методами та прийомами роботи, уміннями та навичками професійного працівника (власне професійна підготовка). На етапі подальшого кваліфікаційного зростання відбувається вирішальний з точки зору особистісної траєкторії подальшого предметного розвитку фахівця процес – регулярне професійне вдосконалення в системі офіційного підвищення кваліфікації та самостійне підвищення рівня ефективності вирішення професійних робочих завдань.

Особливості загальної підготовки (універсального етапу) фахівців у сфері протидії кіберзлочинності. Універсальний етап професійної підготовки полягає в загальній підготовці – засвоєнні аксіоматичних базових життєвих і навчальних орієнтирів та установок, цінних для майбутньої професійної діяльності, а також необхідних теоретичних знань. Так, до загальних і фундаментальних навчальних дисциплін, що вивчаються на факультеті, належать: вища математика, історія України, криміналістика, кримінальне право, кримінальний процес, фізика, філософія тощо. Зрозуміло, що закладання такого роду бази має значення генератора та каталізатора пошуку нових професійно важливих знань і уявлень, а також творчого ставлення до виконання робочих завдань та професійного зростання.

Особливості спеціальної підготовки фахівців у сфері протидії кіберзлочинності: технічний та оперативно-розшуковий напрями, специфіка кожного з них. Окрім фундаментальних, у процесі навчання серед інших навчальних дисциплін залежно від напрямку підготовки курсанти вивчають такі дисципліни технічної та правової спрямованості, як: 1) основи програмування та алгоритмічні мови; 2) основи web-технологій баз та банків даних; 3) теорія інформації та кодування; 4) основи інформаційної безпеки; 5) безпека інформаційних та

комунікаційних систем; 6) криптографія та стеганографія; 7) основи боротьби з кіберзлочинністю; 8) кваліфікація кіберзлочинців; 9) розкриття та розслідування кіберзлочинів; 10) тактико-технічні особливості попередження, розкриття та розслідування кіберзлочинів; 11) технології аудиту інформаційно-телекомунікаційних систем; 12) методи та засоби захисту інформації; 13) захист інформації в банківських системах. Вивчаються також дисципліни суто правоохоронної спрямованості, серед яких: 1) тактико-спеціальна підготовка; 2) спеціальна техніка органів внутрішніх справ; 3) спеціальна фізична підготовка; 4) вогнева підготовка; 5) автомобільна підготовка; 6) режим секретності; 7) оперативно-розшукова діяльність; 8) оперативнотехнічні заходи та негласні слідчі (розшукові) дії.

Отже, випускники факультету відповідно до напрямів підготовки та спеціалізації отримують знання, уміння та навички, що забезпечують: 1) виявлення, попередження та розслідування кіберзлочинів; 2) пошук та аналіз інформації оперативно-розшукового, довідкового та управлінсько-адміністративного характеру в інформаційних системах та мережах; 3) використання інформаційних систем і технологій у роботі правоохоронних органів; 4) забезпечення інформаційної безпеки підрозділів органів внутрішніх справ; 5) технічне забезпечення інформаційно-управляючих систем та комп'ютерних мереж тощо.

Особливості професіоналізації підготовки фахівців у сфері протидії кіберзлочинності. Професіоналізація підготовки фахівців у сфері протидії кіберзлочинності здійснюється шляхом залучення курсантів факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми до роботи навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору (далі – НТЦБКМК), що діє на громадських засадах у Харківському національному університеті внутрішніх справ з 2013 р. Саме в процесі реалізації його функцій курсанти набувають тих знань, умінь і навичок протидії кіберзлочинності, якими вони повинні оволодіти в результаті професійної підготовки, опанують ту професійну компетенцію, що передбачена навчальною програмою та відповідними державними стандартами.

Особливості підвищення кваліфікації (подальшого професійного зростання) в процесі професійної підготовки фахівців у сфері протидії кіберзлочинності. Цікавим, на нашу думку, є виникнення потреби у деяких курсантів – членів колективу навчально-тренувального центру в підвищенні кваліфікації (подальшому професійному зростанні). Подальше професійне зростання нинішнього курсанта, в майбутньому фахівця у сфері протидії кіберзлочинності, відбувається за рахунок вибору ним руху за особистісною траєкторією професійної підготовки та подальшого професійного зростання. Фактично, такого роду розвиток проходить на базі індивідуального навчання та регулярного спілкування з викладачами факультетської кафедри

захисту інформації та стосується лише найбільш підготовлених членів колективу навчально-тренувального центру.

3. *Професійна зорієнтованість навчального процесу.* Одним із найважливіших принципів ми вважаємо також професійну зорієнтованість навчання майбутніх фахівців. З цією метою викладачами факультету розроблена модель практично спрямованого навчання, яка дозволяє вже з другого курсу залучати курсантів до виконання професійних завдань з протидії кіберзлочинності. Така модель організації навчання згодом реально переводить його переважно в професійну площину. Практична спрямованість як важлива складова навчання фахівців у сфері протидії кіберзлочинності починає набувати постійного характеру з другого курсу, коли курсанти освоюють спеціальні знання та уміння, які будуть використовувати у майбутній професійній діяльності.

Навчальний процес на факультеті підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ХНУВС максимально спрямований на послідовне, регулярне формування у курсантів комплексних умінь і навичок, необхідних для успішного виконання майбутніх службових завдань. Для цього до проведення занять залучаються практичні працівники відповідних підрозділів Головного управління Міністерства внутрішніх справ України в Харківській області. Також курсантам передають свої теоретичні знання, практичні уміння та сучасний досвід працівники відповідних підрозділів центрального апарату Міністерства внутрішніх справ України.

Головне місце в забезпеченні професійної зорієнтованості навчального процесу на факультеті належить саме НТЦБКМК («<http://cybercor.in.ua/>»), який надає можливість курсантам під керівництвом кваліфікованих фахівців і самостійно опанувати методи боротьби з кіберзлочинністю та торгівлею людьми. Наприклад, курсанти самостійно створили автоматизований банк даних правопорушень, що відбуваються у всесвітній мережі Інтернет на теренах України. Під час наполегливої цілеспрямованої роботи колектив навчально-тренувального центру, нарощуючи свій досвід і технічний потенціал, дійшов до результативної участі у процесах взаємодії з відповідними службами у цій сфері і зумів зайняти в ній гідне місце. До таких служб належать не тільки Департамент боротьби з кіберзлочинністю та торгівлею людьми МВС України, територіальні органи внутрішніх справ, вищі навчальні заклади системи МВС, а й міжнародні інституції, зацікавлені у налагодженні співробітництва між національними службами боротьби з кіберзлочинністю та підготовці кваліфікованих кадрів для них.

4. *Взаємодія факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми з відповідними практичними підрозділами системи МВС України.* Як уже зазначалося в наших попередніх роботах, найбільш ефективним та якісним

способом вирішення завдань підвищення віддачі від роботи курсантів у НТЦБКМК, а також їх кращої професіоналізації та закріплення стійкої мотивації в обраній сфері діяльності, керівництвом ХНУВС і факультету було обрано налагодження регулярної взаємодії навчально-тренувального центру з Департаментом боротьби з кіберзлочинністю та торгівлею людьми МВС України щодо протидії кіберзлочинності.

За погодженням із відповідними вищестоящими інстанціями ця взаємодія реалізується в різних напрямках і формах, може бути охарактеризована певними видами-формами робіт, що виконують обидві сторони – учасники цієї взаємодії, серед яких:

1. Спільна участь у виконанні обмеженого переліку визначених завдань службової діяльності територіальних підрозділів (з урахуванням рівня складності, режиму секретності тощо), зокрема щодо:

- пошуку в мережі Інтернет інформації, що має протиправний контент, з метою її оперативного виявлення та документування для подальшої роботи;

- розшуку зниклих безвісти дітей (разом з телеканалом «Магнолія-ТВ» і міжнародними неурядовими організаціями на кшталт Міжнародного жіночого правозахисного центру «Ла Страда – Україна»);

- виконання вимог відповідних наказів і рішень колегії МВС України з подальшого вдосконалення виявлення та припинення злочинів, пов'язаних із розповсюдженням протиправного контенту в національному сегменті мережі Інтернет, зокрема № 3509/Рт від 28.02.2013, а також відповідних вказівок і доручень Департаменту боротьби з кіберзлочинністю та торгівлею людьми МВС України.

2. Розробка учасниками роботи навчально-тренувального центру (під час узагальнення досвіду діяльності з указаних вище напрямів) навчально-практичних тренінгів для курсантів вищих навчальних закладів системи МВС України, їх рецензування та подальша апробація за допомогою практичних працівників Департаменту боротьби з кіберзлочинністю та торгівлею людьми МВС і відповідних підрозділів територіальних органів з метою подальшого впровадження в практику повсякденної професійно-службової діяльності [7, с. 8].

Підбиваючи підсумок характеристики форм взаємодії НТЦБКМК з територіальними підрозділами МВС України щодо протидії кіберзлочинності, зазначимо на те, що сутністю та загальною метою поточного функціонування та дослідницької діяльності навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору (на громадських засадах) факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ХНУВС є вихід за рамки стандартного навчального плану та проведення учасниками центру в поза навчальний час практичних і творчих дослідницьких робіт, а також виконання поточних завдань у різних сферах боротьби з кіберзлочинністю, в тому числі у вказаних формах.

Значення знання основних принципів професійної підготовки та їх дотримання в службовій діяльності. Принципи професійної підготовки, як і будь-які інші, мають моральний та будівничий характер. І якщо моральний аспект має оціночне для певного виду діяльності значення, то будівничий – змістовне. Як правило, саме дотримання вимог принципів покликано гарантувати нормальний хід професійної діяльності згідно з визнаними державою стандартами. Крім того, не потрібно забувати, що засвоєння принципів професійної підготовки на етапі навчання з подальшим дотриманням їх у службовій діяльності має велике значення для запобігання професійних деформацій [8]. У підсумку, основні принципи професійної підготовки фахівців виступають як одна з вирішальних умов досягнення справжнього професіоналізму та високих результатів у майбутній діяльності.

Головні завдання роботи колективу НТЦБКМК, її зміст і значення. Для висвітлення функціонування факультетської моделі професійно-орієнтованого навчання зупинимося більш детально на головних завданнях роботи курсантського колективу навчально-тренувального центру. Одним із головних завдань є допомога територіальним підрозділам кримінальної міліції у справах дітей у пошуку безвісти зниклих дітей, які самостійно залишили місце постійного проживання. Учасники НТЦБКМК допомагають практичним працівникам у збиранні за допомогою мережі Інтернет інформації про коло найближчих друзів, імовірне місце знаходження зниклої дитини тощо.

Також члени колективу навчально-тренувального центру за допомогою спеціального програмного забезпечення, що використовується у тому числі й судовими експертами, а також спеціальних адаптерів вчаться досліджувати мобільні телефони як джерело цифрових доказів, тобто виявляти фотографії, відео- та аудіозаписи, що зберігаються на телефоні, контакти власника, відправлені та отримані ним повідомлення тощо (мобільна криміналістика для роботи з логами телефону, історією браузера, картридери для SIM-карток).

Крім того, учасники діяльності НТЦБКМК відпрацьовують методики перевірки стану захищеності персональних комп'ютерів користувачів, серверів, мережевого обладнання та програмного забезпечення у спеціально створеному навчальному кіберсередовищі. Для успішної реалізації цих завдань у розпорядженні навчально-тренувального центру є власний банкомат та POST-термінали, зразки банківських платіжних карток, що використовуються в навчальному процесі для наочного вивчення курсантами пристрою такого типу банківського обладнання. Курсанти мають можливість розглянути принцип їх роботи та можливі методи несанкціонованого доступу, якими користуються зловмисники у своїй злочинній діяльності. Також наявне сканінгове обладнання (накладки на клавіатуру та картприймач банкомату), що використовувалося зловмисниками для незаконного доступу до банківських рахунків потерпілих осіб (скімерське обладнання, зчитувач пластикових карток).

Важливим напрямом діяльності щодо вирішення різноманітних проблем, що проводиться за участі навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору (на громадських засадах) факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ХНУВС, є налагодження постійного співробітництва зі службами МВС відповідного профілю інших країн та міжнародними урядовими та неурядовими організаціями у цій сфері. З 2013 р. міжнародні інституції співпрацюють з МВС України щодо втілення в життя проектів з організації моделі навчання, що полягає в одночасному навчанні та залученні курсантів Харківського національного університету внутрішніх справ до боротьби зі злочинністю, зокрема з таким високотехнологічним її проявом, як кіберзлочинність. Впровадження цієї моделі вже дало вагомий практичний результат: саме завдяки її реалізації вдалося залучити курсантів до здійснення результативного пошуку безвісти зниклих дітей, про що говорилося раніше.

Розвиток цих проектів дозволить також залучити решту вищих системи МВС України, а в майбутньому і цивільних вищих навчальних закладів, до позитивної практики забезпечення правопорядку вже під час навчання. Очевидно, що залучення курсантів, а разом з ними і викладачів, до реальних процесів, які виникають у практичній діяльності правоохоронця, сприяє системному підходу до навчання та акумулює в собі кращі риси сучасної педагогіки. Все це вигідно відрізняє запропоновану модель від існуючих досі традиційних технологій навчання [7, с. 11–12].

Висновки щодо подальшого розвитку та вдосконалення підготовки професійних фахівців у сфері протидії кіберзлочинності. Зазначимо, що кіберзлочинність як в Україні, так і за її межами набуває все більших обертів, тоді як рівень кібербезпеки ще не є досконалим. Тому на сьогодні органам внутрішніх справ дуже потрібні висококваліфіковані фахівці у сфері організації ефективної протидії кіберзлочинцям та захисту службової інформації від несанкціонованого доступу. Випускники факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми більш, ніж випускники будь-яких інших вищих навчальних закладів, мотивовані й професійно підготовлені до службової діяльності в центральному та територіальних підрозділах системи Міністерства внутрішніх справ України, а саме в підрозділах: 1) слідства; 2) боротьби з кіберзлочинністю; 3) експертної служби; 4) оперативно-технічних заходів; 5) інформаційно-аналітичного забезпечення.

Достатньо вагомий результат їх роботи наочно довели ефективність моделі навчально-практичної підготовки, що діє на факультеті підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ХНУВС, і високу якість та перспективність використання існуючих організаційних підходів до роботи з курсантами й надалі. Досвід існуючої взаємодії з територіальними підрозділами

МВС України щодо протидії кіберзлочинності в уособленні цього факультету доводить необхідність подальшого розвитку навчально-тренувального центру протидії кіберзлочинності та моніторингу кіберпростору (на громадських засадах). Цьому може сприяти впровадження нових форм взаємодії з територіальними органами МВС, а також інноваційних форм і методів професійної підготовки фахівців відповідної сфери.

Узагальнюючи досвід діяльності керівництва ХНУВС і факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми щодо методичного забезпечення роботи колективу НТЦБКМК, можна стверджувати, що розвиток міжнародних контактів стає важливим інструментом удосконалення існуючих прийомів роботи у сфері боротьби з кіберзлочинністю, поповнення методичної озброєності вітчизняних служб боротьби з кіберзлочинністю і торгівлею людьми. Враховуючи досвід роботи навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору, можна відзначити, що головним напрямом подальшого поліпшення підготовки фахівців у сфері протидії кіберзлочинності є створення кращих умов для більш успішної професіоналізації курсантів та набуття ними необхідного рівня кваліфікації, потрібної для надійного закріплення професійної мотивації (маємо на увазі більш широке використання матеріальних і моральних засобів стимулювання до праці).

Список використаних джерел: 1. Бандурка О. М. Основи управління в органах внутрішніх справ України: теорія, досвід, шляхи удосконалення : монографія / О. М. Бандурка. – Харків : Основа, 1999. – 440 с. 2. Бандурка О. М. Вищий заклад освіти МВС України : наук.-практ. посіб. / М. І. Ануфрієв, О. М. Бандурка, О. Н. Ярмиш – Харків : Ін-т внутр. справ, 1999. – 369 с. 3. Головатий М. Освіта як соціальний феномен: суть та проблеми подальшого розвитку / М. Головатий // Персонал. – 2010. – № 3–4 (147–148). – С. 176–181. 4. Захожай В. Актуальні питання запровадження навчальних інновацій у вищу освіту / В. Захожай // Персонал. – 2010. – № 3–4 (147–148). – С. 182–187. 5. Лапшина В. Л. Професіоналізм в діяльності органів внутрішніх справ: проблеми теорії та практики : підручник / В. Л. Лапшина. – Харків : Вапнярчук Н. М., 2005. – 224 с. 6. Мирошніченко П. Активні форми навчання персоналу промислових підприємств і студентів / П. Мирошніченко // Персонал. – 2010. – № 1 (145). – С. 62–68. 7. Марков В. В. Форми та методи взаємодії вищих навчальних закладів системи МВС України з територіальними підрозділами МВС щодо протидії кіберзлочинності (на прикладі роботи навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору ХНУВС) / В. В. Марков // Право і Безпека. – 2015. – № 1 (56). – С. 6–14. 8. Марков В. В. Причини, що викликають професійну деформацію працівників ОВС України / В. В. Марков // Право і Безпека. – 2012. – № 4 (46). – С. 226–232.

Надійшла до редколегії 12.10.2015



Марков В. В. Основные принципы подготовки специалистов в сфере противодействия киберпреступности

На примере опыта функционирования модели профессионально-ориентированного обучения, внедрённой на факультете подготовки специалистов для подразделений по борьбе с киберпреступностью и торговлей людьми Харьковского национального университета внутренних дел, охарактеризованы основные организационные и педагогические принципы подготовки специалистов в сфере противодействия киберпреступности, даны рекомендации по её дальнейшему развитию и усовершенствованию.

Ключевые слова: киберпреступность, противодействие киберпреступности, принципы профессиональной подготовки, опережающее обучение, учебно-тренировочный центр по борьбе с киберпреступностью и мониторинга киберпространства, модель профессионально-ориентированного обучения.

Markov V. V. Basic principles of training specialists in combating cybercrime

The article highlights the problem of cybercrime counteraction in Ukraine and basic principles of training specialists in combating cybercrime. The author gives general characteristic of Kharkiv National University of Internal Affairs, the Faculty of Training Specialists in Combating Cybercrime and Human Trafficking and cybercrime combating and cyberspace monitoring training center that was established at the faculty on the voluntary basis. The significance of collaboration of the cybercrime combating and cyberspace monitoring training center with local cybercrime combating units of the Ministry of Internal Affairs of Ukraine as well as with international organizations is emphasized. The description of the basic principles of training specialists in combating cybercrime is provided: availability, methodicalness, complex and systematic character of training. Analyzing the present day situation in Ukraine the author draws a conclusion about the lack of well trained specialists in combating cybercrime in law enforcement agencies and gives recommendations for further improvement of training specialists in combating cybercrime.

Keywords: cybercrime, cybercrime counteraction, principles of professional training, passing ahead studies, cybercrime combating and cyberspace monitoring training center, model of the professionally-oriented studies.

