СТАТТЯ НОМЕРА

УДК [378:351.743(477.54)]:[343.3/.7:004]

В. В. МАРКОВ,
кандидат юридичних наук, старший науковий співробітник,
начальник факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

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)

Під час аналізу форм і методів взаємодії вищих навчальних закладів системи МВС України з територіальними підрозділами МВС у сфері протидії кіберзлочинності надано загальну характеристику Харківського національного університету внутрішніх справ, факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю і торгівлею людьми ХНУВС та навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору (на громадських засадах). Детально описано міжнародний аспект діяльності центру. Внесено пропозиції з метою поліпшення та підвищення ефективності розглядуваної взаємодії.

Ключові слова: *вищі навчальні заклади, Міністерство внутрішніх справ, територіальні підрозділи, методи взаємодії, боротьба з кіберзлочинністю, моніторинг кіберпростору, навчально-тренувальний центр, Харківський національний університет внутрішніх справ.*

Markov, V.V. (2015), "Forms and methods of interaction between higher educational institutions of the Ministry of Internal Affairs of Ukraine and regional divisions of the MIA in the field of cybercrime combating (by the example of the work of Cybercrime Combating and Cyberspace Monitoring Training Center of KhNUIA)" ["Formy ta metody vzaiemodii vyshchykh navchalnykh zakladiv systemy MVS Ukrainy z terytorialnymy pidrozdilamy MVS shchodo protydii kiberzlochynnosti (na prykladi roboty navchalno-trenuvalnoho tsentru borotby z kiberzlochynnistiu ta monitorynhu kiberprostoru KhNUVS)"], *Pravo i Bezpeka*, No. 1, pp. 6–14.

Постановка проблеми. У жодного не викликає сумнівів актуальність боротьби з кіберзлочинністю на сучасному етапі розвитку людства, як і те, що таку боротьбу мають вести фахівці різних галузей виробництва разом із висококваліфікованими фахівцями спеціалізованих правоохоронних органів.

Метою цієї статті є висвітлення окремих питань, що стосуються підготовки у відомчих вищих навчальних закладах (на прикладі Харківського національного університету внутрішніх справ) відповідних кадрів для боротьби з проявами кіберзлочинності, висвітлення напрацьованих і перспективних форм і методів взаємодії ВНЗ системи МВС України з територіальними (практичними) підрозділами МВС із цих питань.

1. Загальна характеристика Харківського національного університету внутрішніх справ і факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми.

Харківський національний університет внутрішніх справ (далі – Університет, ХНУВС) є одним із провідних багатопрофільних вищих навчальних закладів системи Міністерства внутрішніх справ України. Ще в 1993 р. у ньому був створений факультет управління та інформатики, на якому готували фахівців із вищою освітою для системи Міністерства внутрішніх справ України, здатних кваліфіковано розбиратися як у питаннях програмного забезпечення, так і в питаннях правового регулювання суспільних відносин, що виникають у сфері використання інформаційних технологій.

Згодом факультет управління та інформатики було реорганізовано в факультет психології, менеджменту, соціальних та інформаційних технологій, а в 2013 р. на його базі було відкрито факультет підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми (начальник факультету – автор цієї статті). На сьогодні цей факультет – єдиний

в Україні навчальний підрозділ, спеціально створений для підготовки фахівців з протидії кіберзлочинності для системи Міністерства внутрішніх справ України.

Факультет здійснює навчання курсантів за двома напрямами підготовки:

1) «правознавство», що орієнтований на підготовку майбутніх оперативних і слідчих працівників, які працюватимуть у сфері протидії кіберзлочинності та повинні розбиратися у кримінально-правових і процесуальних аспектах розкриття та розслідування злочинів, скоєних з використанням комп'ютерної техніки і технологій (тобто кіберзлочинів);

2) «системи технічного захисту інформації», що орієнтований на підготовку майбутніх оперативних працівників та експертів-криміналістів, які повинні розбиратися в технічних аспектах вчинення кіберзлочинів, документування діяльності кіберзлочинців, а також проведення негласних оперативно-розшукових заходів через кіберпростір і відповідних слідчих дій.

Термін навчання за вказаними напрямами підготовки становить 4 роки.

Випускники факультету відповідно до напрямів підготовки та спеціалізацій отримують знання і навички, що забезпечують:

– виявлення, попередження та розслідування кіберзлочинів;

– пошук та аналіз інформації оперативно-розшукового, довідкового та управлінсько-адміністративного характеру в інформаційних системах і мережах;

– використання інформаційних систем і технологій у роботі правоохоронних органів;

– інформаційну безпеку підрозділів органів внутрішніх справ;

– технічне супроводження інформаційно-управляючих систем та комп'ютерних мереж тощо.

На факультеті проводиться науково-дослідна діяльність із загальнотеоретичних та прикладних питань у галузі інформаційної безпеки та інтелектуальної власності, ведеться робота щодо створення відповідних технологій та методик з протидії кіберзлочинності й торгівлі людьми.

У процесі навчання серед інших навчальних дисциплін залежно від напряму підготовки курсанти також вивчають такі дисципліни технічної та правової спрямованості, як:

– основи програмування та алгоритмічні мови;

– основи веб-технологій баз та банків даних;

– теорія інформації та кодування;

– основи інформаційної безпеки;

– безпека інформаційних та комунікаційних систем;

– криптографія та стеганографія;

– основи боротьби з кіберзлочинністю;

– кваліфікація кіберзлочинів;

– розкриття та розслідування кіберзлочинів;

– тактико-технічні особливості попередження, розкриття та розслідування кіберзлочинів;

– технології аудиту інформаційно-телекомунікаційних систем;

– методи та засоби захисту інформації;

– захист інформації в банківських системах, –

а також навчальні дисципліни правоохоронної спрямованості, а саме:

– тактико-спеціальна підготовка;

– спеціальна техніка органів внутрішніх справ;

– спеціальна фізична підготовка;

– вогнева підготовка;

– автомобільна підготовка;

– режим секретності;

– оперативно-розшукова діяльність;

– оперативно-технічні заходи та негласні слідчі (розшукові) дії.

2. Сутність і форми взаємодії вищих навчальних закладів системи МВС України з територіальними підрозділами МВС щодо протидії кіберзлочинності.

2.1. Характеристика навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору (на громадських засадах).

Навчальний процес на факультеті підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ХНУВС максимально спрямований на посилення практичної складової навчання майбутніх фахівців з протидії кіберзлочинності, послідовного регулярного формування у курсантів комплексних умінь і навичок, необхідних для успішного виконання майбутніх службових завдань.

Зокрема, до проведення лекційних, практичних та лабораторних занять регулярно залучаються практичні працівники відповідних підрозділів Головного управління Міністерства внутрішніх справ України в Харківській області. Крім того, курсантам передають свої теоретичні знання, практичні вміння та сучасний досвід працівники оперативних, слідчих та експертно-криміналістичних підрозділів не тільки територіальних органів, а й центрального апарату Міністерства внутрішніх справ України.

Таким чином під час свого навчання на факультеті курсанти мають змогу опанувати фактично всі існуючі на сьогодні методики

розкриття та розслідування кіберзлочинів, якими користуються у своїй роботі працівники правоохоронних органів України.

З метою посилення практичної спрямованості навчання при факультеті був створений і вже два роки поспіль працює навчально-тренувальний центр боротьби з кіберзлочинністю та моніторингу кіберпростору (на громадських засадах) (далі також – Центр, НТЦБКМК), активними учасниками і консультантами якого стали як курсанти, так і викладачі та працівники ХНУВС. Центр має власну електронну адресу: «http://cybercop.in.ua» [1].

Кваліфікованими працівниками відповідних кафедр факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ХНУВС були розроблені концепція, програма, а також план поточної діяльності Центру, вимогам яких підпорядковується його робота. Зокрема, на виконання вимог такого плану курсанти, які беруть участь у роботі НТЦБКМК самостійно створили програмне забезпечення – автоматизований банк даних про правопорушення, що відбуваються у всесвітній мережі Інтернет на теренах України.

Протягом часу існування Центру навколо його керівництва за відносно короткий термін об'єдналися курсанти, які здатні оволодіти формами та методами його роботи, використовуючи свій власний, вільний від навчання час. Поступово нарощуючи свої інтелектуальні й технічні можливості, колектив НТЦБКМК досяг можливості результативної участі у процесах взаємодії з відповідними службами в цій сфері і, уособлюючи та представляючи Харківський національний університет внутрішніх справ, зумів зайняти гідне місце в ній. Переходячи до описання форм і методів взаємодії зі службами боротьби з кіберзлочинністю, перерахуємо головних суб'єктів цього процесу. До них ми відносимо: Департамент боротьби з кіберзлочинністю та торгівлею людьми МВС України, територіальні органи внутрішніх справ, вищі навчальні заклади системи МВС, а також ті міжнародні інституції, які зацікавлені в налагодженні співробітництва між службами боротьби з кіберзлочинністю та підготовці кваліфікованих кадрів для них. На сьогодні ця взаємодія поки що має двобічний характер, але в майбутньому цілком можливе її розширення на багатосторонній основі із включенням інших суб'єктів, у т. ч. міжнародного права.

2.2. Головні та специфічні форми взаємодії НТЦБКМК з територіальними підрозділами МВС щодо протидії кіберзлочинності.

Як найбільш ефективний та якісний спосіб вирішення завдання підвищення віддачі від роботи курсантів у НТЦБКМК, а також їх кращої професіоналізації та закріплення стійкої мотивації в обраній сфері діяльності керівництвом Університету та факультету було обрано налагодження регулярної взаємодії Центру з Департаментом боротьби з кіберзлочинністю та торгівлею людьми (далі – ДБКТЛ) і відповідними територіальними підрозділами МВС України щодо протидії кіберзлочинності.

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

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 також 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 [2], а також відповідних вказівок і доручень ДБКТЛ МВС України.

2. Розробка учасниками роботи НТЦБКМК (у процесі 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 ДБКТЛ МВС України та відповідних підрозділів територіальних органів з метою подальшого впровадження в практику їх повсякденної професійно-службової діяльності.

До специфічних форм взаємодії Центру з територіальними підрозділами МВС України щодо протидії кіберзлочинності ми відносимо регулярне проведення деяких специфічних для широкого професійного загалу фахівців організаційних заходів у вигляді:

1) особистих зустрічей учасників роботи НТЦБКМК з керівництвом та практичними працівниками відповідних служб центрального апарату МВС України і територіальних органів, зокрема з випускниками ХНУВС, які працюють в них і можуть поділитися набутим досвідом використання знань, умінь і навичок у сфері протидії кіберзлочинності;

2) профільних науково-практичних конференцій з обов'язковою участю в них практичних працівників центрального апарату МВС України, територіальних підрозділів МВС, експертів відповідних неурядових, у т. ч. міжнародних, організацій;

3) більш вузьких за складом учасників, але тематично більш спрямованих методичних семінарів, круглих столів, курсів підвищення професійної кваліфікації тощо.

Вкажемо на те, що на базі Харківського національного університету внутрішніх справ, зокрема із залученням учасників роботи Центру та з урахуванням досвіду його поточної діяльності, проводяться курси підвищення кваліфікації практичних працівників Міністерства внутрішніх справ України, а саме:

– оперативних працівників підрозділів боротьби з кіберзлочинністю;

– слідчих, які займаються розслідуванням злочинів у сфері кіберзлочинності;

– експертів-криміналістів, які спеціалізуються на проведенні комп'ютерно-технічних експертиз та експертиз у сфері захисту інтелектуальної власності.

Підбиваючи підсумок характеристики форм взаємодії Центру з територіальними підрозділами МВС України щодо протидії кіберзлочинності, вкажемо 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 позанавчальний час практичних і творчих дослідницьких робіт, а також виконання поточних завдань у різних сферах боротьби з кіберзлочинністю, в т. ч. за формами, вказаними вище.

3. Методи та зміст взаємодії вищих навчальних закладів системи МВС України з територіальними підрозділами МВС щодо протидії кіберзлочинності.

3.1. Методи взаємодії НТЦБКМК з територіальними підрозділами МВС щодо протидії кіберзлочинності.

Як відомо, методи являють собою алгоритми, які за рахунок відповідних, найбільш раціонально спланованих дій дозволяють успішно виконати завдання, вирішити ту чи іншу проблему, відповісти на питання, як саме досягти поставленої даним суб'єктом мети.

На наш погляд, методи поточної роботи учасників діяльності НТЦБКМК щодо протидії кіберзлочинності з огляду на їх взаємодію з територіальними підрозділами МВС включають у себе тезауруси способів (прийомів, шляхів) вирішення поставлених завдань у певних напрямах:

– *пошуку в мережі Інтернет інформації про осіб, які зникли чи переховуються.* Крім співпраці з практичними підрозділами територіальних органів МВС України, до Центру часто звертаються ті громадяни, які потрапили в надзвичайну ситуацію і потребують кваліфікованої допомоги, наприклад з питань пошуку зниклих дітей *(НЕВІД* (йтиметься далі)*, ресурс Магнолія-ТВ, ресурс МВС «Зниклі безвісти»);*

– пошуку в мережі Інтернет веб-ресурсів, за допомогою яких поширюється інформація або предмети, обіг яких обмежено або заборонено діючим законодавством;

– *дослідження носіїв цифрової інформації (мобільних телефонів та SIM-карток, банківських пластикових карток та скімінгового обладнання тощо).* Члени колективу НТЦБКМК за допомогою спеціального програмного забезпечення, що використовується, у тому числі, судовими експертами, а також спеціальних адаптерів вчаться досліджувати мобільні телефони як джерело цифрових доказів, а саме виявляти фотографії, відео- та аудіозаписи, що зберігаються на телефоні, контакти власника телефону, відправлені та отримані ним повідомлення тощо *(мобільна криміналістика для роботи з логами телефону, історією браузера, картридери для SIM-карток).* У розпорядженні Центру є також власний банкомат та POST-термінали, зразки банківських платіжних карток, що використовуються в навчальному процесі для наглядного вивчення курсантами будови такого типу банківського обладнання. Курсанти мають можливість розглянути принципи їх роботи та можливі методи несанкціонованого доступу, якими користуються зловмисники у своїй злочинній діяльності. Також у наявності є скімінгове обладнання (накладки на клавіатуру та картоприймач банкомату), що використовувалося зловмисниками для незаконного доступу до банківських рахунків потерпілих осіб *(скімерське обладнання, зчитувач пластикових карток);*

– участі в регулярному проведенні масових організаційних заходів для широкого професійного загалу фахівців з протидії кіберзлочинності у вигляді науково-практичних конференцій, тематичних методичних семінарів, круглих столів (у т. ч. телеконференцій з використанням мережі Інтернет в режимі он-лайн), а також курсів підвищення кваліфікації.

До методів взаємодії колективу Центру з територіальними підрозділами МВС щодо протидії кіберзлочинності ми відносимо:

1) спільне обговорення проблем, що виникають у сфері протидії кіберзлочинності, під час виконання поставлених завдань разом з випускниками факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми у складі відповідних робочих груп;

2) обмін досвідом застосування методик, які використовуються у процесі спеціалізованої проблемно-тематичної моніторингової діяльності, тобто спеціально організованого пошуку за ключовими словами тощо.

Крім того, оскільки зміст взаємодії між її учасниками полягає в обміні результатами їх спільної діяльності, до методів взаємодії ми також відносимо регулярне інформування відповідних фахівців територіальних підрозділів боротьби з кіберзлочинністю щодо підозрілих вебресурсів. Зокрема, учасники роботи НТЦБКМК проводять моніторинг світової мережі Інтернет, де виявляють сайти та інші види вебресурсів, на яких розміщено матеріали порнографічного змісту, пропозиції щодо підробки документів, продажу наркотичних, психотропних, вибухових речовин, зброї та інший заборонений відповідно до національного законодавства контент.

Відомості про ці веб-ресурси вносять у спеціальне програмне забезпечення «НЕВІД», розроблене, як вказувалося вище, колективом Центру На базі цього програмного забезпечення розроблений ресурс «Автоматизований банк РОЗШУК», який дозволяє систематизувати всю зібрану інформацію, в тому числі про зниклих дітей, і передавати її на місця, тобто в районні відділи внутрішніх справ МВС України.

Одним із головних завдань роботи НТЦБКМК є допомога територіальним підрозділам кримінальної міліції у справах дітей МВС України у пошуку безвісти зниклих дітей, які самостійно залишили місце постійного проживання. Учасники діяльності Центру допомагають практичним працівникам у збиранні, за допомогою мережі Інтернет, інформації про коло найближчих друзів, ймовірне місце знаходження зниклої дитини тощо.

Підсистема «Автоматизований банк РОЗШУК» використовується також для організації взаємодії між учасниками роботи Центру та практичними працівниками МВС України. Вона дозволяє систематизувати всю зібрану інформацію про зниклих осіб та осіб, які переховуються, та надавати доступ до цієї інформації працівникам територіальних підрозділів міліції.

Один із модулів системи «НЕВІД» акумулює інформацію про правопорушення, що відбуваються у всесвітній мережі на території України. Доступ до системи «НЕВІД» мають працівники територіальних підрозділів боротьби з кіберзлочинністю Міністерства внутрішніх справ України. Для цього в НТЦБКМК налаштований сервер, який підключений до телекомунікаційної мережі МВС України *(спеціальний пошуковий ресурс, розширення для браузера).*

Учасники роботи Центру беруть також участь у дослідженні мережевих вузлів щодо захисту від несанкціонованого проникнення, так званому пентестінгу; відпрацьовують методики перевірки стану захищеності персональних комп'ютерів користувачів, серверів, мережевого обладнання та програмного забезпечення у спеціальному навчальному кіберсередовищі *(nmap – програмне забезпечення для дослідження відкритих мережних сервісів, операційна система Backtrack, Kali Linux).*

3.2. Музей цифрової криміналістики НТЦБКМК та його методичне значення.

Для кращого орієнтування в сучасних тенденціях розвитку цифрової техніки та інших типів обладнання, що може бути використане злочинцями в протиправних цілях, у Центрі зібрано зразки різних типів цифрових носіїв інформації, за допомогою яких учасники його роботи мають змогу опанувати принципи та методи криміналістичного дослідження такого роду джерел цифрових доказів, а також провести порівняння можливостей різних програмно-апаратних комплексів для відновлення видалених файлів та пошуку інформації за ключовими словами на магнітних жорстких дисках, флеш-носіях тощо.

Такі зразки становлять фондову колекцію музею цифрової криміналістики НТЦБКМК колекції тематичних зібрань якого експонуються та поповнюються з кожним днем. Отримані технічні засоби використовуються не тільки як музейні експонати, що наочно демонструють розвиток цифрових інформаційних технологій, але й як навчальні прилади під час проведення практичних і лабораторних занять з навчальних дисциплін, викладення яких пов'язане з отриманням знань та навичок у сфері цифрової

криміналістики і, таким чином, має неабияке методичне значення.

Наразі в експозицію музею цифрової криміналістики входять зразки:

1) sim-карток операторів мобільного (стільникового) зв'язку;

2) мобільних (стільникових) телефонів різних поколінь;

3) пластикових банківських карток:

– з магнітною стрічкою;

– зі SMART-чипом;

– комбінованих;

4) накопичувачів на жорстких магнітних дисках:

– для стаціонарних комп'ютерів;

– для ноутбуків;

5) застарілих цифрових фотоапаратів та цифрових відеокамер;

6) Flash-носіїв:

– флеш-карток до мобільних телефонів та цифрових фото- й відеокамер;

– USB-носіїв;

7) мережевого та комунікаційного обладнання:

– модемів для дротових телефонних ліній;

– ADSL-модемів;

– мережевих комутаторів та концентраторів;

– Wi-Fi-адаптерів;

– Wi-Fi точок доступу;

8) сканерів відбитків пальців рук.

Фондова колекція музею цифрової криміналістики отримала схвальні відгуки багатьох гостей НТЦБКМК – вітчизняних і міжнародних експертів у сфері боротьби з кіберзлочинністю. Плідно використовуючи подекуди його унікальні експонати, курсанти–учасники роботи Центру поряд із вирішенням навчальних завдань мають у своєму розпорядженні інструментарій, завдяки якому наочно відпрацьовують ті методики, які використовують практичні працівники МВС України під час проведення слідчих дій, оперативно-розшукових заходів, експертних досліджень та експертиз.

3.3. Міжнародний аспект роботи колективу НТЦБКМК факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ХНУВС.

Важливим напрямом діяльності з вирішення різноманітних проблем, у якому бере участь НТЦБКМК 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 в цій сфері.

Зауважимо, що під час зустрічей з іноземними фахівцями є можливість вирішення важливих методичних проблем у сфері боротьби з кіберзлочинністю та підготовки кадрів. Зокрема, в 2014 р. регіональним офісом ОБСЄ в Україні в рамках співпраці з Харківським національним університетом внутрішніх справ та реалізації проекту «Посилення боротьби з торгівлею людьми та кіберзлочинністю в Україні» був організований візит до Університету старшого інспектора-слідчого з кіберзлочинів служби по боротьбі з організованою злочинністю Департаменту боротьби з кіберзлочинністю Міністерства внутрішніх справ Сербії Любана Петровича. Метою візиту цього міжнародного експерта було проведення оцінки потреб у підвищенні кваліфікації та посиленні (посилення) матеріально-технічної бази факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ХНУВС. У результаті робочого візиту від Любана Петровича було отримано кваліфіковані об'єктивні оцінки рівня кваліфікації учасників роботи НТЦБКМК, оснащення його технічної бази, якості програмного забезпечення, перспективи на майбутнє щодо взаємодії з міжнародними організаціями, в т. ч. у справі підготовки кваліфікованих кадрів. Підбиваючи підсумок свого візиту, Любан Петрович акцентував увагу на тому, що міжнародні установи зацікавлені у підвищенні професійності українських правоохоронців у сфері протидії кіберзлочинності, оскільки боротьба з кіберзлочинністю – це міжнародна проблема, яка потребує об'єднання зусиль усіх цивілізованих країн.

Так, наприклад, у рамках Меморандуму про взаєморозуміння між урядом України та урядом Сполучених Штатів Америки щодо допомоги з правоохоронних питань Харківський національний університет внутрішніх справ відвідали представники Посольства США в Україні та Міжнародної програми підвищення кваліфікації для органів кримінального розслідування ICITAП Департаменту юстиції Сполучених Штатів Америки. Також на базі ХНУВС Американською асоціацією юристів «Ініціатива з верховенства права в Україні» (ABA ROLI Україна) проводилися тренінги для працівників слідчих та оперативних підрозділів щодо особливостей застосування комп'ютерних технологій під час розслідування кіберзлочинів. Під час зустрічі старший консультант з правоохоронних питань регіонального програмного офісу ICITAП Департаменту юстиції США Роберт Пікок зазначив: «Ми шукаємо можливості співпраці з вашим університетом та розвитку

факультету, який готує фахівців по боротьбі з кіберзлочинністю».

Починаючи з 2013 р., ІСІТАП посилено співпрацює з МВС України щодо впровадження в життя проектів з організації моделі навчання, яка полягає в одночасному навчанні та залученні курсантів Харківського національного університету внутрішніх справ до боротьби зі злочинністю, зокрема з таким високотехнологічним її проявом, як кіберзлочинність. Упровадження такої моделі навчально-практичної підготовки має велике соціальне та практичне значення. Вже сьогодні завдяки її реалізації вдалося залучити курсантів до попередження реальних злочинів, а також здійснити результативний пошук безвісти зниклих дітей.

Розвиток цих проектів дозволить також залучити решту вузів системи МВС України, а у майбутньому і цивільних вищих навчальних закладів до позитивної практики забезпечення правопорядку під час навчання. Це є водночас як цікавим для курсантів і студентів, так і корисним для суспільства. 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 вирізняє запропоновану модель. Зазначену модель навчально-практичної підготовки Харківський національний університет внутрішніх справ висував на здобуття Державної премії України в галузі освіти 2014 року [3].

Частими гостями факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ХНУВС є не тільки керівники та працівники правоохоронних органів України, але й іноземці та представники міжнародних організацій, які займаються питаннями організації протидії кіберзлочинності та торгівлі людьми, а також питаннями допомоги її жертвам.

У рамках взаємодії з Міжнародним жіночим правозахисним центром «Ла Страда – Україна» Харківський національний університет внутрішніх справ займається адмініструванням «Електронної гарячої лінії» з протидії дитячій порнографії в Інтернеті», на веб-сайт якої (internetbezpeka.org.ua) від користувачів мережі Інтернет надходить інформація про факти створення та розповсюдження дитячої порнографії в Інтернеті та за його межами, про факти рекламування або пропонування послуг дитячого секс-туризму на території України, а також щодо жорстокого поводження з дітьми. Курсанти, які беруть участь у роботі НТЦБКМК, під керівництвом працівників ХНУВС обробляють інформацію, що надходить, та передають її до компетентних підрозділів Міністерства внутрішніх справ України.

Можна стверджувати, що розвиток міжнародних контактів чим далі, тим більше стає важливим інструментом удосконалення існуючих методів роботи у сфері боротьби з кіберзлочинністю, перспективним напрямом подальшого поповнення методичної озброєності вітчизняних служб боротьби з кіберзлочинністю та торгівлею людьми.

Виходячи з досвіду роботи навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору (на громадських засадах) факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ХНУВС та аналізу наведених вище методів, можна відмітити, що головним змістом його взаємодії було і є:

1) створення умов для більш успішної професіоналізації курсантів та набуття ними необхідного рівня кваліфікації, потрібної для надійного закріплення професійної мотивації вже на стадії навчання шляхом раннього безпосереднього включення в рішення деяких поточних завдань професійно-службової діяльності посильного для учасників роботи рівня складності;

2) підготовка, особливо в особі найбільш мотивованих учасників роботи навчально-тренувального центру, достатньо кваліфікованих фахівців до ефективної участі в міжнародному співробітництві у сфері протидії кіберзлочинності та торгівлі людьми.

4. Висновки та пропозиції щодо поліпшення та підвищення ефективності взаємодії вищих навчальних закладів системи МВС України з територіальними підрозділами МВС з питань протидії кіберзлочинності.

У підсумку зазначимо, що, по-перше, оскільки кіберзлочинність набуває все більших обертів, а рівень кібербезпеки, існуючий в Україні, поки що залишає бажати кращого, висококваліфіковані фахівці у сфері протидії кіберзлочинності є вкрай цінною штатною одиницею будь-якого практичного підрозділу, і саме тому наразі органам внутрішніх справ необхідні кваліфіковані кадри для організації ефективної протидії кіберзлочинцям та захисту службової інформації від несанкціонованого доступу.

По-друге, випускники факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ХНУВС затребувані та працюють у різних територіальних

практичних підрозділах системи Міністерства внутрішніх справ України, в тому числі у центральному апараті Міністерства, а саме в підрозділах: слідства; боротьби з кіберзлочинністю; експертної служби; боротьби зі злочинами, пов'язаними з торгівлею людьми; оперативно-технічних заходів; інформаційно-аналітичного забезпечення тощо. Достатньо вагомі результати їхньої роботи наочно довели ефективність моделі навчально-практичної підготовки, що діє на факультеті, та високу якість і перспективність використання існуючих організаційних підходів до роботи з курсантами й надалі.

Водночас досвід існуючої взаємодії між вищими навчальними закладами системи МВС України з територіальними підрозділами МВС щодо протидії кіберзлочинності в уособленні факультету відповідної спрямованості доводить необхідність подальшого розвитку та вдосконалення цієї діяльності, зокрема в межах роботи навчально-тренувального центру протидії кіберзлочинності та моніторингу кіберпростору (на громадських засадах), що фактично вже має доволі висококваліфікований професійний характер.

Актуальність вирішення нагальних проблем у сфері підвищення рівня інформаційної безпеки в нашій країні настійно вимагає пошуку інноваційних результативних і разом з тим ефективних рішень. Цьому може сприяти впровадження та освоєння нових форм і видів взаємодії вищих навчальних закладів з територіальними органами МВС, а також інноваційних форм і методів навчання (педагогічних технологій) генерації кадрів працівників правоохоронної сфери, здатних опановувати сучасні підходи до підвищення рівня загальної самоосвіти, спеціалізації та кваліфікації.

З метою поліпшення та подальшого підвищення ефективності взаємодії вищих навчальних закладів системи МВС України з територіальними підрозділами МВС щодо протидії кіберзлочинності у майбутньому, на нашу думку, не тільки потрібне, але й можливе вдосконалення існуючої взаємодії в такого роду напрямах і формах:

1) підвищення кваліфікації колективу навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору (на громадських засадах), в тому числі за рахунок регулярного стажування у вітчизняних (в центральній і територіальних) службах боротьби з кіберзлочинністю та міжнародного обміну досвідом роботи;

2) розширення кола учасників взаємодії, її багатостороння основа (включаючи вітчизняні та міжнародні урядові й неурядові організації в цій сфері);

3) чітке визначення кола проблем, що мають бути вирішені за участю колективу навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору (на громадських засадах) у сфері боротьби з кіберзлочинністю; планове та поступове нарощування складності поставлених завдань;

4) розвиток міжнародного співробітництва з практичними службами боротьби з кіберзлочинністю Міністерств внутрішніх справ високорозвинених країн світу, неурядовими організаціями з надання допомоги жертвам торгівлі людьми (в т. ч. у сфері сексуальної експлуатації); налагодження регулярного обміну досвідом практичної спрямованості навчання майбутніх фахівців по боротьбі з кіберзлочинністю та торгівлею людьми із закордонними навчальними закладами аналогічного профілю підготовки, включаючи стажування та обмін кадрами викладачів і курсантів (студентів).

Список використаних джерел

1. Навчально-тренувальний центр боротьби з кіберзлочинністю та моніторингу кіберпростору на громадських засадах : [сайт] / Харків. нац. ун-т внутр. справ, Ф-т підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми [Електронний ресурс]. – Режим доступу: http://cybercop.in.ua.

2. Про стан виявлення та припинення злочинів, пов'язаних із розповсюдженням протиправного контенту в національному сегменті мережі Інтернет : рішення розшир. наради керівництва МВС України від 28.02.2013 № 3509/Рт. – 2 с. – Служб. док.

3. Про підтримку кандидатів на здобуття Державної премії України в галузі освіти 2014 року[1] : лист Міжнар. програми підвищення кваліфікації для органів кримінал. розслідування (ICITAP) М-ва юстиції США міністру освіти і науки України та ректору Харків. нац. ун-ту внутр. справ від 22 квіт. 2014 р. – 2 с. – Служб. док.

[1] У листі підтримано проект з організації моделі навчання, яка полягає в одночасному навчанні та залученні курсантів Харківського національного університету внутрішніх справ до реальних процесів, які виникають у практичній діяльності правоохоронця, зокрема в боротьби з кіберзлочинністю.

4. Угода про спільну діяльність [між Управлінням боротьби з кіберзлочинністю МВС України, Управлінням кримінальної міліції у справах дітей МВС України та Харківським національним університетом внутрішніх справ] : від 20 листоп. 2013 р. – 2 с. – Служб. док.

5. Law Enforcement Training Strategy : Project area specific strategies : Draft version, 5 Aug. 2014 [Електронний ресурс] / Prepared under the GLACY project // Council of Europe : [сайт] / Directorate General Human Rights and Rule of Law. – P. 67. – Режим доступу: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/GLACY/Reports/2688_4_4_LEA_Training_Strategy_report_v4_PUBLIC.pdf. – Рішення про включення Харків. нац. ун-ту внутр. справ до Стратегії Ради Європи «Підготовка правоохоронних органів» в частині навчання фахівців з протидії кіберзлочинності в Україні (серпень 2014 р.).

6. Харківський національний університет внутрішніх справ : [сайт] / Харків. нац. ун-т внутр. справ, Інформац.-техн. від. [Електронний ресурс]. – Режим доступу: http://www.univd.ua.

7. Харківський національний університет внутрішніх справ / за заг. ред. С. М. Гусарова. – Харків : [б.в.], 2015. – 352 с. : іл.

Надійшла до редколегії 13.05.2015

МАРКОВ В. В. ФОРМЫ И МЕТОДЫ ВЗАИМОДЕЙСТВИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ СИСТЕМЫ МВД УКРАИНЫ С ТЕРРИТОРИАЛЬНЫМИ ПОДРАЗДЕЛЕНИЯМИ МВД В ВОПРОСАХ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ (НА ПРИМЕРЕ РАБОТЫ УЧЕБНО-ТРЕНИРОВОЧНОГО ЦЕНТРА БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ И МОНИТОРИНГА КИБЕРПРОСТРАНСТВА ХНУВД)

При анализе форм и методов взаимодействия высших учебных заведений системы МВД Украины с территориальными подразделениями МВД в по вопросам противодействия киберпреступности предоставлена общая характеристика Харьковского национального университета внутренних дел, факультета подготовки специалистов для подразделений борьбы с киберпреступностью и торговлей людьми ХНУВД и учебно-тренировочного центра борьбы с киберпреступностью и мониторинга киберпространства (на общественных началах). Детально описан международный аспект деятельности центра. Внесены предложения с целью улучшения и повышения эффективности рассматриваемого взаимодействия.

Ключевые слова: *высшие учебные заведения, Министерство внутренних дел, территориальные подразделения, методы взаимодействия, борьба с киберпреступностью, мониторинг киберпространства, учебно-тренировочный центр, Харьковский национальный университет внутренних дел.*

MARKOV V. V. FORMS AND METHODS OF INTERACTION BETWEEN HIGHER EDUCATIONAL INSTITUTIONS OF THE MINISTRY OF INTERNAL AFFAIRS OF UKRAINE AND REGIONAL DIVISIONS OF THE MIA IN THE FIELD OF CYBERCRIME COMBATING (BY THE EXAMPLE OF THE WORK OF CYBERCRIME COMBATING AND CYBERSPACE MONITORING TRAINING CENTER OF KHNUIA)

The article deals with the analysis of forms and methods of interaction between higher educational institutions of the Ministry of Internal Affairs of Ukraine and regional divisions of the Ministry of Internal Affairs of Ukraine in the field of combating cybercrime. The author outlines the work of Kharkiv National University of Internal Affairs, the Faculty of Training Specialists in Combating Cybercrime and Human Trafficking of KhNUIA and Cybercrime Combating and Cyberspace Monitoring Training Center founded there on the voluntary basis. The role of action-oriented training at the Faculty of Training Specialists in Combating Cybercrime and Human Trafficking is emphasized; the training is aimed at the development of knowledge and skills necessary for future law enforcement officers to fulfill their duty assignments.

The article provides extensive coverage of the work of Cybercrime Combating and Cyberspace Monitoring Training Center, the forms of its interaction with regional divisions of the Ministry of Internal Affairs of Ukraine and the center's international activity.

The conclusions are drawn and proposals are forwarded as to the improvement of methods and forms of interaction between higher educational institutions of the Ministry of Internal Affairs of Ukraine and regional divisions of the Ministry of Internal Affairs of Ukraine in order to raise effectiveness of cybercrime counteraction.

Keywords: *higher educational institutions, Ministry of Internal Affairs, regional divisions, methods of interaction, cybercrime combating, cyberspace monitoring, Kharkiv National University of Internal Affairs.*