УДК 343.985.7

**О. ВОЛКОВ**, ад’юнкт Київського національного університету внутрішніх справ

# ДО ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ ПРАВООХОРОННИХ ОРГАНІВ ПО БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

***Анотація.*** *Щодо організації навчального процесу з підготовки фахівців правоохоронних органів для протидії злочинності в сфері інформаційних технологій; представлені форми підготовки, методика закріплення практичних навичок.*

*Актуальність проблеми*, яка подається до розгляду, полягає в належній забезпеченості відповідними фахівцями правоохоронних органів та їх підготовки в сфері протидії несанкціонованому втручанню за допомогою шкідливих програмних засобів в електронно-обчислювальні машини (комп’ютери), автоматизовані системи, комп’ютерні мережі та мережі електрозв’язку, а також в комплектації таких органів фахівцями в сфері інформаційних технологій та захисту інформації. Вирішення проблеми підготовки фахівців і комплектування правоохоронних органів певною мірою задовольнить потреби як науки (теоретичні розробки захисту інформації), так і практики (захист інформації як предмета злочинного посягання) та буде сприяти підвищенню ефективності захисту інформації в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах та мережах електрозв’язку, ефективного викриття, документування, розкриття та розслідування злочинів у цій сфері. Розробка практичних дієвих заходів щодо протидії проявам злочинної діяльності в сфері інформаційних технологій і адекватного реагування на такі злочини є важливим завданням сьогодення.

*Мета цієї публікації* – висвітлення результатів наукових досліджень стосовно підготовки спеціалістів для правоохоронних органів по боротьбі зі злочинами в сфері інформаційних технологій.

Дослідженням питання підготовки фахівців у сфері інформаційних технологій приділяється увага у наукових статтях, періодичних наукових виданнях та монографіях. Безпосередньо цю проблеми вивчали: Романюк Б.В., Гавловський В.Д., Гуцалюк М.В., Іщенко А.В., Цимбалюк В.С., Белкін Р.С., Хахановський В.Г., Біленчук П.Д. та інші вчені, які займалися розробкою питання протидії кіберзлочинності. Незважаючи на розгляд даної проблематики з боку вчених, автором публікації пропонується свій погляд та пропозиції щодо конструктивного вирішення проблеми комплектації правоохоронних органів фахівцями.

У відомчих вищих навчальних закладах системи МВС на даний час розроблені і активно вивчаються слухачами та курсантами навчальні програми з розслідування комп’ютерних злочинів. Донецький інститут внутрішніх справ, що є навчальним закладом саме такого спрямування [7], проводить навчання співробітників МВС з розслідування злочинів у сфері інформаційних технологій [8], а також організації оперативно-розшукової роботи на основі інформаційних технологій [9]. У Харківському національному університеті внутрішніх справ у цьому плані фахівцям після закінчення навчального закладу видають два дипломи про вищу освіту за спеціалізаціями: “правознавство” – “слідчо-криміналістична” і “захист інформації з обмеженим доступом та автоматизація її обробки – організація захисту інформації”.

Слід відмітити навчальні дисципліни у вищому державному навчальному закладі

МВС України IV рівня акредитації (Київський національний університет внутрішніх справ) на здобуття юридичної освіти за спеціальністю “правознавство” (7.060101). Цей заклад актуалізував навчальний процес, і слухачам слідчої спеціалізації пропонувалося здобуття знань, пов’язаних з інформаційною безпекою: інформатизація управління в ОВС (108 годин); комп’ютеризовані інформаційні системи правоохоронних органів та інформаційна безпека (72 години); криміналістична інформатика (108 годин). В цьому ж навчальному закладі за спеціальністю “управління у сфері правопорядку” (8.000004) освітньо-професійної програми підготовки магістрів пропонується курс: криміналістична інформатика (27 годин).

Певної підготовленості слідчих підрозділів вимагають і відомчі нормативні акти МВС України. Так слідчий повинен не лише вміти ефективно працювати з організаційною, криміналістичною, спеціальною технікою і засобами зв’язку [10], а й знати та дотримуватись заходів інформаційної безпеки. На жаль в цьому документі не вказано не тільки про впровадження в практичну діяльність слідчих підрозділів таких специфічних програмних засобів, як АРМ “Слідчий” чи АРМ “Керівник слідчого підрозділу”, а й про навчання користування розробками щодо інформаційної безпеки. Практичну цікавість слідчих підрозділів в цьому плані викликають не вищезазначені програмні засоби, які б значно спростили роботу слідчого і керівника слідчого підрозділу, а програмні засоби “підтримки прийняття рішень” в конкретних ситуаціях. В теоретичному ж плані про ці розробки слідчим відомо лише з оглядових відомчих джерел та лекційних занять, практично ж вони не використовуються через їх ненадходження в практичні підрозділи районних відділів області.

В слідчому відділенні, де працює автор, проводиться робота по спрощенню документообігу процесуальних документів, які складаються під час розслідування кримінальних справ. В цьому напрямі проведена робота по створенню бази стандартних процесуальних бланків розроблених ГСУ МВС України [11], яка заповнюється в програмі Microsoft Office Excel по кожній кримінальній справі. Спрощення роботи при використанні цієї бази даних полягає в напівавтоматичному заповненні процесуально значущих фактів, обставин та подій по кожній кримінальній справі. Після закінчення проведення досудового розслідування по кожній кримінальній справі залишається повне наглядове провадження в електронному вигляді бази даних а не окремих процесуальних документів. В цій же програмі співробітниками СУ УМВС розроблені бланки та логіка до заповнення місячних та квартальних звітів СЛ та СЛМ, які певною мірою полегшують роботу при складанні звітності керівників слідчих підрозділів.

У структурі Державного департаменту боротьби з економічною злочинністю МВС України створено спеціальний підрозділ по боротьбі з правопорушеннями у сфері інформаційних технологій. В Державному науково-дослідному експертно-криміналістичному центрі створено відділ криміналістичних комп’ютерних досліджень з проведення таких експертиз. З 2007 р. відповідно до Закону України “Про Державну службу спеціального зв’язку та захисту інформації України” від 23 лютого 2006 року завдання, пов’язані із захистом інформації (зокрема, участь у формуванні та реалізації державної політики у сфері захисту інформаційних ресурсів, створення та розвиток систем технічного та криптографічного захисту інформації), вирішуватиме Державна служба спеціального зв’язку та захисту інформації України. В системі МВС аналогічні функції покладені на Департамент документального забезпечення та режиму. Один з напрямів діяльності цього департаменту – захист інформації технічними засобами, зокрема убезпечення комп’ютерного обладнання від несанкціонованого втручання [12].

Діяльність щодо спрощення роботи, пов’язаної з документообігом, ведеться і в самому центральному апараті МВС. Так в 2006 р. фахівці Департаменту документального забезпечення та режиму почали працювати над впровадженням електронного документообігу по Міністерству внутрішніх справ у цілому та в регіонах аби повністю позбутися паперової частини діловодства. Відбулася презентація програмних продуктів трьох фірм, які брали участь в розробці цього проекту. Спільно з Департаментом інформаційних технологій розроблені технічні вимоги і завдання до такого програмного комплексу. У системі буде задіяний центральний апарат, далі електронний зв'язок сягатиме обласних управлінь і далі райвідділів міліції.

Для об’єднання всіх канцелярій в самому центральному апараті міністерства в одну систему необхідно створити 150 робочих місць. Взагалі ж по Україні впровадження комп’ютерного документообігу потребує відповідного сертифікованого оснащення разом з програмним забезпеченням, а також додатково 1500 фахівців [13].

Відповідно до Закону України “Про основи національної безпеки України” [14] наша держава реалізує комплексну програму по усуненню загроз національній безпеці в різних сферах, в тому числі й в інформаційній. Пріоритетним напрямом цієї діяльності є комп’ютерна злочинність та комп’ютерний тероризм. Без сучасного захисту інформації в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах та мережах електрозв’язку не може бути забезпечена національна безпека нашої держави.

У зв’язку з цим постає проблема не тільки браку самих знань, а й кадрового забезпечення підрозділів професіоналами. Відомчі навчальні заклади системи МВС України проводять підготовку фахівців правоохоронних органів у сфері боротьби з кіберзлочинністю. Але така підготовка не повною мірою відповідає потребам сьогодення та оперативної обстановки в регіонах.

Проблеми вищої освіти в Україні з підготовки фахівців у сфері інформаційних технологій неодноразово досліджувались у фахових виданнях. Це і низька заробітна плата професорсько-викладацького складу, практична відсутність матеріального забезпечення навчального процесу, дефіцит сучасної навчальної літератури, відірваність від світових джерел наукової інформації у сфері боротьби з кіберзлочинністю. Вихід з такої ситуації вбачається в розробці загальнодержавної програми підготовки фахівців. На думку інших дослідників, основним недоліком процесу підготовки фахівців називається відсутність єдиної стратегії боротьби з цими злочинами та безсистемність в організації процесу підготовки та перепідготовки кадрів у цій сфері [15].

Підготовку фахівців у сфері інформаційних технологій необхідно продовжувати у напряму реформування діяльності відомчих закладів освіти МВС України з підготовки та перепідготовки фахівців: оперативних співробітників, слідчих, експертів. Постійно проводити перегляд навчальних планів, введення таких предметів, як правова інформатика та інформаційне право, а також нових спеціалізацій з інформаційно-аналітичного забезпечення діяльності ОВС, захисту відомчої інформації і боротьби з кіберзлочинністю. Освітньо-професійні плани навчання повинні входити до затверджених галузевих стандартів вищої освіти, тобто визначення сучасних напрямів підготовки фахівців по боротьбі з кіберзлочинністю.

Такий фахівець повинен мати належну підготовку не тільки з юридичних дисциплін, а й природничо-наукових: фізики, математики, інформатики, достатніх для розв’язання завдань у сфері боротьби з комп’ютерною злочинністю, знання обчислювальних середовищ, прикладних програм, технічних аспектів організації захисту інформації.

Метою курсу спеціальних дисциплін професійної підготовки є формування не тільки практичних навичок, а й професійного світогляду фахівця з інформаційної безпеки: систематичне, теоретичне і практичне опанування класифікації шкідливих програмних засобів, слідову картину такої злочинної діяльності, мотивів, способів захисту інформації, виявлення каналів несанкціонованого проникнення за допомогою шкідливих програмних засобів, встановлення особи злочинця, класифікація методів і способів заміни, знищення, блокування, перехоплення, копіювання комп’ютерної інформації та комплексне вивчення такої злочинної діяльності.

Для практичного закріплення теоретичних знань курс дисципліни супроводжується розрахунковими та курсовими роботами, проектами, ціллю яких є вироблення практичних навичок проектування і розроблення систем захисту в сучасних умовах. При цьому необхідно звертати увагу саме на вивчення практичних навичок, що є результатом теоретичної підготовки.

В цьому плані в навчальних закладах системи МВС є плідні напрацювання. На кафедрі військового тилу Академії ВВ МВС було створено лабораторію автоматизації. На її базі в 1998 р. створено окремий підрозділ – інформаційно-обчислювальний центр (ІОЦ). У його структурі три відділення: програмного забезпечення, технічного обслуговування обчислювальної техніки та інформаційного забезпечення. В Академії налічується 208 ПЕОМ, з яких 128 використовуються у навчальному процесі. Обладнано 12 навчальних комп’ютерних класів, створено локальну мережу з доступом до Інтернету.

У повсякденній діяльності Академії використовуються програмні продукти, створені власними фахівцями: веб-сторінка Академії, АРМ “Оперативний черговий”, АРМ “Матеріальні цінності тилу”, АРМ “Автотранспорт”, АРМ “Оповіщення”, електронний каталог методкабінету, програми “Грошове забезпечення офіцерів, прапорщиків та курсантів”, “Розкладка продуктів”, “Система обліку успішності”, “Система тестування”, “Система створення екзаменаційних білетів”. У грудні 2005 року було розроблено та впроваджено автоматизовану систему навчальних матеріалів “АСУНМ” [16].

Дещо по-іншому поставлена робота прокуратур районів області. Так, широкого поширення знайшла інформаційно-аналітична система “Прокурор”, призначена для складання та автоматизованої обробки статистичних звітів в органах прокуратури України. В районних прокуратурах Чернігівської області в практичному користуванні знаходиться база даних нормативних документів “Нормативні акти України” (розробник ЗАТ “Інформтехнологія”); внесення змін до нормативних актів проводиться регулярно і дане питання стоїть на контролі обласної прокуратури. Широке застосування необхідним програмним продуктом районних прокуратур тісно пов’язано з належним забезпеченням комп’ютерним обладнанням, комп’ютерними мережами, розмножувальною апаратурою [17]. Керівний апарат обласної прокуратури усвідомлює необхідність впровадження сучасних інформаційних технологій. Тому що, як наголошується іншими дослідниками, розвиток підсистеми інформаційної безпеки є важливою складовою стратегії системної інформатизації прокуратури України [18].

Використання інформаційних технологій проводиться не тільки в практичній роботі а й у навчальному процесі при підвищенні кваліфікації прокурорсько-слідчих кадрів Академії прокуратури України. Зокрема, матеріальна база навчального закладу дає змогу ефективно проводити навчання з використанням сучасних технічних можливостей: новітніх засобів електронного зв’язку, сучасної комп’ютерної і оргтехніки, передового програмного забезпечення [19]. Сучасні навчальні аудиторії і

відповідне їх оснащення повною мірою дають змогу слухачам засвоювати необхідні знання.

Ефективною робота прокуратур районів буде лише при використанні можливостей комп’ютерних правових програм, впровадженні сучасних технологій отримання, обробки, зберігання і систематизації інформації. Наявна технічна база дає змогу постійного поновлення комп’ютерних правових програм, ведення картотеки нормативних актів, автоматизації обробки статистичної інформації [20]. Використання засобів електронного зв’язку в прокуратурах має певну специфіку (насамперед це пов’язано з захищеністю цих каналів) і вимагає від прокурорських працівників вмінь та навичок користування засобами інформаційної безпеки і каналами електронного зв’язку. Прикладом організації таких мереж може стати електронна мережа, якою користуються органи внутрішніх справ. Це віртуальна комп’ютерна мережа, яку на правах оренди ВАТ “Укртелеком” (монополіст усіх дротовних телекомунікацій) виділяє УМВС по областях. Тобто за договором акціонерне товариство виділяє свої канали зв’язку для користування ОВС. Така мережа має свої як переваги, так і недоліки. Основною перевагою в цьому плані є захищеність каналів зв’язку від несанкціонованого втручання як самими технічними засобами ВАТ “Укртелеком”, так і технічним персоналом УМВС області, рух всієї інформації в мережі знаходиться під контролем співробітників відділу інформаційних технологій.

У сучасних умовах співробітники правоохоронних органів не можуть достатньою мірою тримати в полі зору всі технічні нововведення, що стрімко розвиваються в інформатиці. Готуючи таких співробітників, одним з основних завдань, на нашу думку, є відслідковування новітніх інформаційних технологій, розробка нових методик захисту інформації з застосуванням таких методик на практиці.

Недоліком у розробці методик інформаційної безпеки є те, що методика розкриття та розслідування злочинів, документування, проведення експертиз після проведення необхідних досліджень і обґрунтувань втрачає свою актуальність та своєчасність застосування. Це пов’язано певним чином з так званим феноменом “старіння інформації”, а також з тим, що такі методики розробляються як наслідок злочинної діяльності, а тому самі злочинні прояви (так як це і є новітні інформаційні технології, які на півкроку попереду навіть найсучасніших систем захисту та методик розслідування цих злочинів) можуть ще не мати ефективної протидії. Виходом із цієї ситуації може бути постійний аналіз злочинних проявів у сфері інформаційних технологій, дослідження властивостей та функцій шкідливих програмних засобів, вивчення практичного досвіду фахівців зарубіжних країн у сфері розслідування та проведення комп’ютерних експертиз, вивчення слідової картини, залишеної шкідливим програмним засобом унаслідок несанкціонованого втручання в роботу комп’ютерів, автоматизованих систем, комп’ютерних мереж та мереж електрозв’язку. Дослідження процесу створення шкідливих програмних засобів їх використання, розповсюдження і збуту, криміналістичне забезпечення практичної діяльності може набувати форму обзорів, довідок, методичних рекомендацій, довідникових посібників.

Автором з метою з’ясування рівня інформаційної культури було проведено анкетування співробітників районного відділу внутрішніх справ України. В результаті 88,8 % опитаних працівників ОВС зазначили, що не мають досвіду роботи в розкритті і розслідуванні злочинів, пов’язаних з виготовленням, розробкою, поширенням і збутом шкідливих програмних засобів. Цей стан речей може засвідчувати, що такий вид злочинів не має широкого поширення або ж високий ступінь його латентності. На думку автора, така ситуація склалася внаслідок масового поширення різного роду програмних

систем захисту (антивіруси, фаєрволи, програмні комплекси, спрямовані на виявлення шкідливих програмних засобів і процесів, що загрожують стабільності і функціональності інформаційних систем). Та недостатня правова освіченість користувачів електронної інформації про захист їх інтересів з боку держави і про кримінальну відповідальність за створення, використання, розповсюдження і збут шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу комп’ютерів, автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку [22], приводить до латентності такого виду злочинів у силу ряду причин. В практичному аспекті кожен з користувачів персональним комп’ютером неодноразово зустрічався з тими чи іншими шкідливими програмними засобами, а звернення з цього питання в правоохоронні органи носять поодинокий характер.

Під час вивчення результатів опитування бралися до уваги фактори, які зумовлюють низьку ефективність діяльності правоохоронних органів у цій сфері. Опитані респонденти зазначили кілька, на їх думку, суттєвих факторів:

- відсутність знань, розуміння технологічного процесу роботи комп’ютерів (55,5 %);
- відсутність розроблених сучасних методик виявлення та розслідування створення, використання, розповсюдження і збуту шкідливих програмних засобів (50 %);
- новизна таких злочинів, недостатня обізнаність про способи їх вчинення (44,4 %);
- недостатня професійна компетентність та неукомплектованість оперативних працівників (38,8 %).

Опитані співробітники РВ УМВС (100 %) зазначили про необхідність спеціального вивчення тактики злочинців щодо створення, використання, розповсюдження і збуту шкідливих програмних засобів. Результат відповідей саме на це питання свідчить про практичну зацікавленість правоохоронців у вивченні тактики протиправної діяльності з метою ефективної протидії таким злочинним проявам. 94,4 % опитаних повідомили про недостатність методичних рекомендацій, оглядів, літератури стосовно боротьби з шкідливими програмними засобами, призначеними для несанкціонованого втручання в роботу комп’ютерів, автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку. Про недостатність розроблених методик може свідчити те, що Головним слідчим управлінням в 2002 р. розроблена методика “Розслідування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж” [22], якою до даного часу користуються практичні працівники. Сучаснішими розробками ця методика не поновлювалась, не говорячи про надходження інших методик у сфері інформаційних технологій в практичні підрозділи.

При з’ясуванні у працівників ОВС джерела інформації про злочини в сфері інформаційних технологій 72,2 % опитаних відповіли, що цим джерелом є обмін досвідом і знаннями з колегами, і лише 22,2 % вказали на службову підготовку і підвищення кваліфікації. Ця проблема не є новою для МВС, і питанням її вирішення постійно приділяється увага. З метою виправлення ситуації, яка склалася в практичних підрозділах ОВС, запроваджено практику цільових виїздів до головних управлінь, УМВС з метою перевірки фахових знань співробітників у цій сфері та надання практичної допомоги. Аналогічну роботу проведено в ряді структурних підрозділів центрального апарату МВС. Проведено семінари та навчальні збори з працівниками служб та іншими підрозділами щодо поліпшення діяльності по захисту інформації і каналів зв’язку [12].

Іншим напрямом виходу з цієї ситуації є налагодження зв’язків навчальних закладів МВС з практичними органами. Цей процес повинен бути двостороннім із взаємною зацікавленістю як навчальних закладів, так і замовників-спеціалістів. Цікавим

прикладом зворотного зв'язку у навчанні може бути Прикарпатський юридичний інститут Львівського державного університету внутрішніх справ. Потреби практики активно вивчаються у вигляді: проведення курсів підвищення кваліфікації працівників різних служб, а також керівників міськрайвідділів. При навчанні практичних співробітників вивчаються і в подальшому враховуються побажання щодо корисності і своєчасності наукових розробок. Узагальнення таких пропозицій проводиться шляхом анкетування [23]. Десь в чомусь схожа підготовка слідчо-прокурорських працівників Академією прокуратури України, яка проводиться на високому професійному рівні співпраці з Академією правових наук та іншими науковими і навчальними закладами України, країн СНД та ЄС [24]. Така діяльність провідного навчального закладу прокуратури налагоджена і розвивається у сфері наукових досліджень, видавничої діяльності, обміну досвідом з підвищення кваліфікації та підготовки кадрів прокурорських працівників.

Підготовка фахівців, які протистоять кіберзлочинності повинна проводитись з урахуванням міжнародного досвіду зарубіжних правоохоронних органів, досягнень у протидії такого виду злочинів. Накази Генеральної прокуратури України чітко зазначають міжнародне співробітництво в роботі органів прокуратури, мета якого – удосконалення механізмів та процедур надання правової допомоги й обміну досвідом, встановлення й розвиток контактів з компетентними установами іноземних держав і міжнародними організаціями [25]. Практичний бік цього співробітництва реалізується у вигляді зустрічей, переговорів, конференцій, семінарів, реалізації проектів і програм співпраці.

Вивчивши потреби практики, вищі навчальні заклади повинні мати сучасні навчальні програми для слідчих, оперативних та експертних підрозділів, готувати фахівців відповідно до державного замовлення цим органам. Необхідно уважно вивчати вимоги підрозділів, що ведуть боротьбу з несанкціонованим втручанням в роботу комп’ютерів, автоматизованих систем, комп’ютерних мереж та мереж електрозв’язку. Необхідність підготовки фахівців у сучасних умовах полягає в тому, що сама сфера інформаційних технологій розвивається стрімкими темпами, розробляються та впроваджуються нові системи для передачі даних, технічні стандарти та інше.

Крім цього, при підготовці фахівців необхідно звертати увагу і на зміни законодавства в даній сфері. Відповідно до ст. 35 Європейської конвенції про кіберзлочинність від 23 листопада 2001 р. ратифікованої Верховною Радою України 7 вересня 2005 р. необхідно створити спеціальний орган, який зміг би координувати роботу щодо протидії кіберзлочинності для цілодобових контактів з метою надання негайної допомоги в розслідуванні чи переслідуванні кримінальних правопорушень, пов’язаних з комп’ютерними системами і даними, або з метою збирання доказів в електронній формі, що стосується кримінального правопорушення [26]. При створенні такого органу знову таки постає проблема наповнюваності його необхідними фахівцями для забезпечення виконання покладених функцій.

Такий погляд ученого на розроблювану програму, пов’язану з протидією злочинності в сфері інформаційних технологій, вимагає від вищих навчальних закладів підготовки фахівців як в кількісному, так і в якісному співвідношенні. Оперативно реагуючи на потреби цих органів, на думку автора, можливе створення індивідуальних планів підготовки слухачів та курсантів останніх курсів на замовлення практичних органів.

Певну увагу в цьому необхідно приділяти організації практики слухачів та курсантів таких підрозділів. Така практика повинна бути тісно пов’язана з місцем

розподілу молодих фахівців, що дасть змогу випускнику після закінчення вищого навчального закладу усвідомити застосування цих практичних навичок під час навчання. Перебуваючи на переддипломній практиці, майбутній фахівець об’єктивно оцінює фахову підготовку та свої якості в майбутній практичній діяльності.

Зрозуміло, що керівники таких підрозділів хочуть мати добре підготовленого спеціаліста і, бажано, з досвідом оперативної роботи за фахом. Але такими випускники стають лише після тривалої роботи протягом 2 – 3 років під наглядом досвідчених керівників. Тобто досвід приходить тільки з практичним застосуванням теоретичних знань, і найпростіший шлях отримання кваліфікованих працівників – через переддипломну практику та стажування на посаді.

Накази МВС України з метою підвищення фахового рівня слідчих системи МВС України регламентують різні види навчання. В контексті розгляду проблемного питання, пов’язаного з відсутністю розробленої методики запобігання такого виду злочинам, як створення, використання, розповсюдження і збут шкідливих програмних засобів, слід звернути увагу на такий вид навчання, як перепідготовка, підвищення кваліфікації, функціональна підготовка [27]. Цей вид навчання проводиться у вищих навчальних закладах МВС України, інститутах, на факультетах, курсах підвищення кваліфікації і перепідготовки інших міністерств і відомств, в училищах професійної підготовки ГУМВС, УМВС, ГУДСО, навчальних центрах підготовки, за місцем роботи.

Певна відмінність існує у навчанні прокурорсько-слідчих кадрів. Так якісне навчання цих кадрів закріплене наказами Генеральної прокуратури України [28] і зобов’язує щоквартально проводити навчально-методичні семінари, висвітлення в фахових виданнях позитивного досвіду розслідування окремих категорій злочинів, використання можливостей судових експертиз та інших проблемних питань.

Вищі ж навчальні юридичні заклади при підготовці кадрів для прокуратур розробляють навчальні програми з урахуванням практичних потреб прокурорсько-слідчої практики [29].

На думку автора, необхідно підняти статус магістра. Фактично на сьогодні склалася ситуація, що слухачі та курсанти не мають бажання продовжувати навчання в магістратурі і вважають за краще швидше закінчити вищий навчальний заклад у якості спеціаліста. Це пов’язано з тим, що немає різниці у фахових знаннях при отриманні диплома спеціаліста чи магістра і з відсутністю зацікавленості практичних підрозділів у фахівцях з повною вищою освітою. На даний час намічені перспективи розв’язання цієї проблеми, в результаті приєднання України до Булонського процесу та використання в навчальному процесі перспективної кредитно-модульної технології.

В практичній діяльності правоохоронних органів, що протидіють злочинності в сфері інформаційних технологій, позитивні результати показали фахівці, що навчались у вищих навчальних закладах України, які готують спеціалістів для радіоелектронної промисловості, таких як Національний технічний університет України “КПІ”, Харківський державний технічний університет радіоелектроніки, Львівський національний університет, Одеський національний політехнічний університет, Севастопольський національний технічний університет, Державний університет інформаційно-комунікаційних технологій та ін. Підготовка фахівців проходить із спеціалізованим вивченням технологічних і технічних питань захисту інформації та протидії несанкціонованому втручанню в роботу комп’ютерів, автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку. Тому є сенс в підготовці магістрів і спеціалістів, які мають юридичну освіту, у цих вищих навчальних закладах за державним замовленням правоохоронних органів з урахуванням специфіки подальшої

професійної діяльності. Цей процес з боку держави необхідно взяти під контроль та належним чином організувати, викликаючи зацікавленість в подальшому навчанні у магістратурах за вузькопрофільною спеціалізацією.

Актуальною проблемою в підготовці спеціалістів, що займаються боротьбою із злочинністю у сфері інформаційних технологій, є збереження та поповнення викладацьких кадрів, підтримання їх на належному професійному рівні. Не останнє місце в матеріально-технічному забезпеченні навчального процесу займає поповнення таких кафедр талановитою молоддю, створення умов для їх ефективного навчання в сфері інформаційних технологій, належне забезпечення кафедр та навчальних аудиторій комп’ютерною технікою, підвищення заробітної плати викладацькому складу відповідно до професійних здобутків, якостей з підготовки та проведення навчального процесу.

**Висновки.**

1. Реалії сьогодення вимагають від держави вжити своєчасні й адекватні заходи з протидії злочинності в сфері інформаційних технологій. Суттєвим кроком у цьому напрямі може стати розробка і прийняття загальнодержавної програми підготовки таких фахівців.

2. На належному рівні забезпечити навчальний процес для таких фахівців. Це і матеріальне забезпечення майбутніх фахівців сучасною навчальною літературою не тільки вітчизняних, а й зарубіжних авторів. Забезпечення інформацією щодо передових інформаційних технологій та розробок у сфері захисту інформації. Забезпечення доступу до зарубіжних джерел наукової інформації.

3. Залучати до підготовки таких фахівців як досвідчений професорсько-викладацький склад, так і практичних співробітників. Організація поповнення кафедр молодими спеціалістами, що мають як теоретичні, так і практичні напрацювання в цій сфері. Забезпечення гідної оплати їх діяльності та матеріального забезпечення.

4. Моніторинг навчальних планів, інформаційно-аналітичного забезпечення навчального процесу саме з урахуванням розвитку інформаційних технологій, напрямку злочинних проявів та протидії такій злочинності. Спрямувати таку підготовку на вивчення не тільки в гуманітарній а й в природничо-науковій сфері, тобто не тільки технічне виявлення слідової картини, а й профілактике кіберзлочинів.

5. Стимулювати в процесі навчання майбутніх фахівців такий вид практичної діяльності як розрахункові, курсові роботи та проекти захисту інформації, метою яких є саме закріплення практичних навичок. Постійно проводити відслідковування розробок і здобутків сучасної радіоелектроніки, комп’ютерних технологій у формі обзорів, довідок, методичних рекомендацій, довідникових посібників.

6. Спрямувати таку підготовку не тільки на вміння застосування здобутих практичних навичок, а й на формування професійного світогляду майбутнього фахівця.

7. Організація навчального процесу повинна відповідати потребам практичних правоохоронних органів, готувати фахівців відповідно до державного замовлення та потреб сьогодення з урахуванням передових інформаційних технологій, що розвиваються стрімкими темпами. За необхідності впровадити в навчальний процес індивідуальних планів підготовки на замовлення практичних органів.

8. Для здобуття необхідних практичних навичок майбутні фахівці повинні проходити переддипломну практику та стажування на посаді безпосередньо в тому практичному органі, за направленням якого вони навчали і в подальшому будуть працювати.

9. Приєднання України до Булонського процесу, впровадження європейських стандартів вищої освіти у вітчизняних навчальних закладах значно змінять ставлення до професійної вищої освіти, підвищать статус магістрів, рівень і якість отримуваних знань.

## Використана література

1. Сандул І. В мережі // Кореспондент. – 2006. – № 30/219. – С. 45.

2. Романюк Б.В., Гавловський В.Д., Гуцалюк М.В. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: практичний посібник. – К., 2004. – С. 144.

3. //www.cybersecurity.ru.

4. Р.Семеха. Проблема міжнародного масштабу / Міліція України. – № 5(119)2007. – С. 7.

5. //www.ukranews.com.

6. Львовски М. Два самых крутых крымских хакера учились еле-еле, но украли семь месяцев интернет-времени / Сегодня, 14.04.2005 р. – С. 23.

7. Титунина Е.В. Донецке готовят киберполицейских. – (Центр исследования компьютерной преступности //www.crime-research.ru/news/16.02.2005/1813.

8. Маклаков Г.Ю., Рижков Є.В. Методологічні підходи до вдосконалення підготовки кадрів ОВС з урахуванням розвитку інформаційних технологій. – У кн.: Проблеми правознавства та правоохоронної діяльності: зб. наукових статей: Вид-во ДІВС МВС України. – 2001. – № 2. – С. 121-133; Маклаков Г.Ю., Рыжков Э.В. Методология подготовки кадров МВД с учетом развития современных информационных технологий. – В кн.: Информационные технологии и информационная безопасность в науке, технике и образовании “ИНФОТЕХ-2002”: материалы Международ. науч.-практ. конф. (30 сентября – 5 октября 2002 г., К.-Севастополь): НТО РЭС Украины, 2002. – С. 109-110.

9. Маклаков Г.Ю., Рыжков Э.В. Особенности оперативно-розыскной деятельности при расследовании преступлений в сфере высоких технологий. – У кн: Використання сучасних досягнень криміналістики у боротьбі зі злочинністю: матеріали міжвуз. наук.-практ. конф. студентів, курсантів і слухачів (Донецьк, 12 квітня 2002 року). – Донецьк: ДІВС, 2002. – С. 19-29; Маклаков Г.Ю. Возможности современных информационных технологий при проведении криминалистических исследований и экспертиз. – У кн: Використання сучасних досягнень криміналістики у боротьбі зі злочинністю: матеріали міжвуз. наук.-практ. конф. студентів, курсантів і слухачів (Донецьк, 12 квітня 2002 року). – Донецьк: ДІВС, 2002. – С. 342-355.

10. Наказ МВС України № 160 від 20.02.2006 р. (додаток № 6).

11. Зразки бланків процесуальних та інших документів у кримінальній справі: практичний посібник; Під редакцією В.І.Захарова. – К., 2002 р.

12. Стешенко Л. Гончаров О. Канцелярія без стосів паперу: мрія чи реальність? / Іменем Закону. – 2007 р. – № 10. – С. 6-7.

13. Там же. – С. 6-7.

14. Закон України від 19.06.2003 р. № 964-IV “Про основи національної безпеки України”.

15. Підготовка фахівців у сфері інформаційної безпеки: стан в Україні. К.І. Бєляков, В.Д. Гавловський // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2005. – № 12 //mndc.naiau.kiev.ua/Gurnal/12.htm.

16. Романчук П. Інформаційні технології: від джерел до сучасності / Іменем Закону. – 2007. – № 18-19. – С. 20.

17. Наказ ГП України від 22.04.2004 року № 7 гн “Про організацію роботи з питань правового забезпечення в органах прокуратури”.

18. Цимбалюк В. Щодо формування стратегії інформатизації прокуратури України в умовах розвитку інформаційного суспільства // Вісник прокуратури. – 2007. – № (71). – С. 97.

19. Наказ № 2/3 гн ГП України від 30.09.2004 р. “Про вдосконалення організації роботи щодо підвищення кваліфікації прокурорсько-слідчих кадрів в Академії прокуратури України”.

20. Наказ № 1/3 гн ГП України від 19.09.2005 р. “Про організацію роботи з питань первинного обліку, ведення статистичної звітності в органах прокуратури та нагляду за обліком злочинів”.

21. Закон України “Про внесення змін до Кримінального та Кримінально-процесуального кодексів України” // Відомості Верховної Ради України. – 2005. – № 6. – Ст. 261-262.

22. Збірник методичних рекомендацій з питань розкриття та розслідування злочинів слідчими та оперативними працівниками ОВС; за редакцією П.В. Коляди. – К., 2002. – С.101-127.

23. Голинський І. Наука зайняла свою нішу в інституті / Міліція України. – 2007. – № 4. – С. 24-25.

24. Наказ ГП України від 11.11.2005 р. № 2/3 “Про внесення змін до наказу від 30 вересня 2004 р. № 2/3 гн” (п. 6.2).

25. Наказ ГП України від 26.12.2005 р. № 8 гн “Про організацію роботи органів прокуратури України у галузі міжнародного співробітництва і правової допомоги“ (п.п. 2.2).

26. Гуцалюк М.В. Міжнародне співробітництво щодо протидії злочинам у сфері інформаційних технологій // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2003. – № 8. – С. 97-104.

27. Наказ МВС України № 1444 від 25.11.2003 р. “Про організацію професійної підготовки осіб рядового і начальницького складу органів внутрішніх справ України”.

28. Наказ ГП України від 19.09.2005 р. № 4 гн “Про організацію прокурорського нагляду за додержанням законів органами, які проводять дізнання та досудове слідство” (п.п. 1.3; 11, 16).

29. Наказ ГП України від 8.10.2004 р. № 2/4 гн “Про вдосконалення організації роботи з добору абітурієнтів для вступу до базових вищих навчальних закладів” (п. 1.4).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~