ДЕРЖАВНА СЛУЖБА: АСПЕКТИ ТА ПРАКТИКИ

УДК 343.98

О. В. ОРЛОВ, Ю. М. ОНИЩЕНКО

ДЕРЖАВНА ПОЛІТИКА ПІДГОТОВКИ КАДРІВ З ПОПЕРЕДЖЕННЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

***Р**озглянуто питання підготовки кадрів по боротьбі з кіберзлочинністю як складової держаної політики в галузі боротьби зі злочинами з використанням інформаційних технологій. Надано пропозиції щодо підготовки спеціалістів у галузі попередження кіберзлочинності в державі.*

Ключові слова: кіберзлочин, кібербезпека, фахівці, загроза, інформаційні технології, державна стратегія.

***T**he issue of training staff to combat cybercrime, as part of state policy in the field of crime control with the use of information technologies has been considered. Proposals are given as for training specialists in prevention of cybercrime in the country.*

Key words: cybercrime, cyber security, specalists, threat, information technologies, state strategy.

Кібернетична злочинність має не лише правову і технічну, але і соціальну проблему, ефективне рішення якої вимагає, насамперед, системного підходу з розробки основ забезпечення безпеки життєво важливих інтересів держави, суспільства і громадянина в кіберпросторі.

Під системою протидії кібернетичної злочинності прийнято розуміти взаємоузгоджену діяльність органів державної, виконавчої влади, організацій і підприємств усіх форм власності за такими напрямами:

– дослідження, аналіз і оцінка кібернетичних загроз, форм і методів її організації, а також рівня кібернетичної безпеки в реальних умовах інформатизації держави і суспільства;

– удосконалення чинного законодавства з питань кібернетичної безпеки відповідно до міжнародних норм на рівні ООН, НАТО, Інтерполу, Європейського Союзу та ін.;

– здійснення ефективних заходів попередження, розслідування і протидії кібернетичним злочинам;

– підготовка фахівців у галузі кібернетичної безпеки та боротьбі з кіберзлочинністю.

Технічна складова всіх можливих видів злочинів є однаковою і не залежить від того, чи йде мова про злочини проти конституційних прав особи, майнових прав людини, злочинів в економічній сфері або проти громадської і державної безпеки. Виходячи з цього, технічна складова підготовки фахівців у галузі кібернетичної безпеки також є однаковою і не залежить від відомчих компетенцій у питаннях забезпечення кібернетичного захисту держави, суспільства і особи.

Проблематика попередження злочинності та підготовки кадрів у сфері інформаційних технологій і кіберебезпеки досить часто обговорюється фахівцями у сфері новітніх технологій, інформаційної безпеки та державного управління в журналах, на конференціях, круглих столах і засобах масової інформації. Деякі аспекти попередження кіберзлочинності вивчали та обговорювали у своїх статтях К. Бєляков, С. Битко, В. Бутузов, А. Волеводз, В. Голубєв, Д. Дубов, С. Кльоцкін, В. Мілашев, М. Литвинов, В. Мохор, Е. Рижков, Т. Тропіна, В. Хахановський та інші.

Аналіз наукової літератури засвідчив, що при всій значущості теми розвитку державного регулювання боротьби з кіберзлочинністю в Україні та підготовки фахівців у даній галузі, вона вивчена ще не в повному обсязі. На сьогодні вітчизняними вченими опубліковано та обговорено недостатньо наукових праць, що досліджують цю проблематику. Зокрема, не дістала належного висвітлення державна політика підготовці кадрів з попередження кіберзлочинності в Україні.

Мета статті – дослідити та проаналізувати проблеми, які виникають при підготовці фахівців з боротьби з кіберзлочинністю як складовою державної політики в галузі боротьби зі злочинами з використанням новітніх інформаційних та телекомунікаційних технологій, надати пропозиції щодо покращання ситуації з попередженням кіберзлочинності в країні.

Вплив інформаційних загроз на структури державної влади, які відповідальні за підготовку і ухвалення рішень, реалізація яких безпосередньо впливає на безпеку країни, може призводити до виникнення надзвичайних ситуацій в державі і суспільстві, значним збиткам із-за порушення функціонування систем зв'язку, контролю і управління та просочування інформації, яка містить державну таємницю.

Слід зазначити, що не існує загальноприйнятого визначення кіберзлочинності. У різних країнах в це поняття вкладають різний сенс. За визначенням ООН кіберзлочинність – має на увазі будь-який злочин, який може бути здійснений з використанням комп'ютерної системи або мережі, в рамках або проти комп'ютерної системи або мережі. Таким чином, до кіберзлочинів може бути віднесено будь-який злочин, здійснений в електронному середовищі. Злочин, здійснений е кіберпросторі, – це протиправне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні дії, здійснені за допомогою комп'ютерів, комп'ютерних мереж і програм.

Нині законодавством України поняття “кіберзлочинність” безпосередньо не визначено. Європейська Конвенція про кіберзлочинність також не надає конкретного формулювання, хоча і визначає низку суспільно небезпечних діянь, які повинні мати статус кіберзлочинів на рівні національного законодавства. До них відноситься сукупність злочинів з використанням комп'ютерних систем і технологій, таких як незаконний доступ до комп'ютерної системи, нелегальне перехоплення даних, втручання в дані, правопорушення, пов'язані з дитячою порнографією, що в цілому відповідає положенням Конвенції про кіберзлочинність [1].

Статистика свідчить, що наша країна є одним з лідерів за кількістю кібератак у всьому світі. Україна виявилася у цієї сфері на четвертому місці після Росії, Тайваню і Німеччини [2]. Це відбувається тому, що українська законодавча база, що регулює питання існування кіберпростору і злочинів з використанням інформаційних технологій, недостатньо розроблена і впроваджена. У зв'язку з цим хотілося б відмітити таке. В Україні в якості кіберзлочинів передбачені і закріпленні в окремому розділі XVI Кримінального кодексу України [3] суспільно небезпечні діяння “Злочину у сфері використання електронний – обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку”. До кіберзлочинів відносяться як: традиційні злочини, що здійснюються за допомогою комп'ютерних технологій і інтернету (шахрайство з використанням ЕОМ, незаконний збір відомостей, що становлять комерційну таємницю, шляхом несанкціонованого доступу до комп'ютерної інформації тощо), так і такі що, стають можливими завдяки новітнім комп'ютерним технологіям.

Аналіз існуючих підходів до побудови процесу підготовки фахівців у сфері захисту інформації в США, країнах Західної Європи і в деяких державах СНД дозволив виділити домінуючі напрями і сконцентрувати увагу на розгляді існуючих підходів до процесу навчання.

У США найсерйознішу увагу приділяють проблемі підготовки фахівців для захисту національних інформаційних структур. Проведений аналіз освітніх програм із захисту інформації в США, доступних на сайтах вищих навчальних закладів показує, що найбільш затребуваними освітніми програмами (з мірою бакалавр), як і у Великобританії, є розслідування комп'ютерних інцидентів, далі за популярністю серед американських студентів – інформаційна безпека, комп'ютерна безпека, безпека комп'ютерних мереж. Також у США студенти мають можливість отримати освіту за програмами в галузі інформаційної безпеки з присудженням ступеня Master of Business Administration.

Важливо відмітити, що в США багато уваги приділяється привертанню громадської уваги до проблеми інформаційної безпеки. У 1998 р. у рамках федерального бюро розслідувань було створено Національний центр захисту інфраструктури (NIPC), який об'єднує представників органів влади, військових і приватного сектора, для захисту національних інфраструктур.

На NIPC покладено ключову роль у забезпеченні безпеки інформаційних систем. За задумом він повинен стати свого роду мозковим центром, покликаним займатися аналітикою і координувати дії інших розвідувальних і контррозвідувальних служб [4].

Міжнародна асоціація фахівців з комп'ютерних досліджень (IACIS) забезпечує навчання у сфері комп'ютерних технологій. Організація займається поширенням інформаційних програм і проведенням заходів, спрямованих на боротьбу з кіберзлочинністю. Успішно функціонує Національний союз кібербезпеки, створений спільно урядом і промисловцями США. Мета союзу – розробка підходів до проблеми безпеки в кіберпросторі, підвищення рівня освіти у сфері інформаційної безпеки, привертання громадської уваги до проблеми кібертероризму.

Проведений огляд присвячених підготовці фахівців у США дозволив виділити найбільші компанії, що проводять навчання у сфері інформаційної безпеки: Cisco Systems, Check Point Software Technologies, IBM, , Internet Security Systems, Microsoft, Sun Microsystems, Symantec. Серед навчальних центрів, що спеціалізуються на підготовці фахівців із захисту інформації, можна відмітити: CERT, GIAC, Cisco Systems, CSI.

Для вдосконалення методів навчання в Міністерстві оборони створено спеціальний підрозділ – "Управління програм по інформаційній безпеці (Information Assurance Program Office" [5]. Агентство національної безпеки (NSA) сформувало низку центрів Postgraduate освіти та підключило до них провідні університети США.

У зв'язку з різким переходом систем управління на IT-рішення відчувається нестача фахівців у сфері інформаційної безпеки. І в нашій країні така необхідність зростає набагато швидше, ніж йде підготовка відповідних кадрів.

З урахуванням широкого використання можливостей кіберпростору для здійснення вже відомих і передбачених кримінальним кодексом злочинів, виникає необхідність удосконалення системи протидії кіберзлочинності, розмежування компетенцій правоохоронних і інших державних органів у питаннях вказаної протидії.

На порядок денний знову виноситься теза про створення системи підготовки, перепідготовки і підвищення кваліфікації співробітників відповідних держструктур.

У той же час необхідно відмітити, що вчені в процесі оцінювання стану комп'ютерної злочинності часто посилаються на дані інших країн, для яких питання кібербезпеки украй актуальні, зважаючи на критичну залежність їх управлінської інфраструктури від відповідних інформаційних систем і мереж.

З урахуванням багатоаспектності цієї проблематики, її виходу за межі вузькоспрямовнного сприйняття комп'ютерних інцидентів як IT-спеціалістами, так і правоохоронцями, особливе значення набуває зміст підготовки відповідного персоналу. Головною метою освіти повинне стати

формування розуміння неприпустимості комп'ютерних інцидентів і високої громадської небезпеки їх наслідків. Передусім, потрібна базова освіта у сфері ІТ-технологій. Але вона не повинна дублювати спеціалізовані курси системних адміністраторів і програмістів.

Доцільно прислухатися до думок ІТ-спеціалістів при розробці відповідних нормативно-правових актів. Також корисними виявляються знання у сфері узагальнення матеріалів розслідувань і розгляду в судових інстанціях відповідних матеріалів, по яких ІТ-фахівці залучалися як експерти і консультанти [6].

Адже проблеми дослідження комп'ютерних інцидентів можна вирішити і вирішувати надалі тільки за тісної взаємодії всіх зацікавлених представників держави і суспільства.

Проблема підготовки кадрів для боротьби з кіберзлочинністю опрацьовується в Україні з кінця 1990-х рр. Безумовно, позитивні тенденції в роботі з підбору, відбору і навчанню такого персоналу є – деякі кіберзлочини вже викриваються. Проте статистика вітчизняних правоохоронців з викриття кіберзлочинів, неадекватна існуючим в Україні кіберзагрозам. Більш того, багато країн серйозно висловлюються про необхідність ідентифікації певних кібератак як фактів воєнних дій. У зв'язку з цим потрібна подальша робота із внесення змін до вітчизняного карного законодавства з урахуванням міжнародних норм і стандартів, а також неприпустимо ігнорування фактами здійснення з території нашої держави подібних кібердій. Зауважимо, що кіберзлочини відносяться до так званих "тихих" злочинів. Мало того, що зловмисник намагається бути непомітним, він ще й маскує сліди своїх дій. Тому дієва боротьба з кіберзлочинами неможлива без системного моніторингу усього кіберпростору.

Безумовно, в Україні за останні десять років накопичено певний досвід протидії кіберзлочинності як у практичному, науковому і навчально-методичному плані. Одночасно слід зазначити недостатню координацію управлінських рішень у цьому питанні на всіх рівнях і значну відособленість навчальних програм і наукових досліджень, які велися в країні в цей період.

При всьому цьому головна проблема – підготовка кваліфікованих кадрів у цьому напрямі і забезпечення ними практичних підрозділів – з кожним роком все чіткіше набуває міжвідомчого характеру, оскільки сама кіберзлочинність з вузьковідомчого статусу реально виходить на рівень проблеми національної безпеки.

За останні десять – п'ятнадцять років трансформувалися паралельно понятійно-категоріальний апарат цієї галузі знань, вітчизняне законодавство, система підрозділів правоохоронних органів і сама кіберзлочинність. За всіма позиціями тенденція має чітко виражений міжнародний характер.

Отже, і перспективи, очікувані в майбутньому правоохоронними органами Україні, можна спрогнозувати з великою мірою ймовірності. Кіберзагрози набувають з кожним роком усе більш глобального характеру.

Для того щоб мінімізувати прорахунки в боротьбі з кіберзлочинністю, необхідно визнати раніше допущені помилки і внести в уже існуючу стратегію зміни, які ґрунтуються на наших, передусім вітчизняних, реаліях і позитивному міжнародному досвіді.

Стосовно системи органів внутрішніх справ основними проблемними питаннями формування відомчої кіберінфраструктури є:

– відсутність чіткої стратегії створення і розвитку спеціалізованих підрозділів по боротьбі з кіберзлочинністю;

– розрізненість зусиль практичних і навчальних підрозділів з питань підготовки відповідних кадрів;

– відсутність резерву кандидатів для комплектування відповідних підрозділів і посад по лінії роботи;

– відсутність належного представництва провідних фахівців практичних підрозділів на спеціалізованих науково-практичних заходах;

– досить популістський підхід у питаннях організації співпраці основних суб'єктів боротьби з кіберзлочинністю;

– відсутність єдиного центру підготовки і перепідготовки кадрів для боротьби з кіберзлочинністю (оперативний склад, слідчі, експерти).

За умов реформування системи вищої освіти в Україні організація такої підготовки є складним завданням, виконанню якого повинне сприяти створення системи цільової підготовки і перепідготовки фахівців у сфері протидії кіберзлочинності.

У Харківському національному університеті внутрішніх справ у 2013 р. створено факультет підготовки фахівців для підрозділів по боротьбі з кіберзлочинністю і торгівлею людьми, який здійснює підготовку таких кадрів: слідчих, які спеціалізуються на розслідуванні кіберзлочинів; оперативних працівники для підрозділів боротьби з кіберзлочинністю; експертів у науково-дослідних експертно-криміналістичних центрах, що проводять експертні дослідження комп'ютерної техніки та програмних продуктів, телекомунікаційних систем (обладнання) та засобів, відеозвукозапису, а також у сфері інтелектуальної власності. Випускники факультету відповідно до напрямів підготовки і спеціалізацій отримують знання і навички, засвоюють методи і засоби, що забезпечують розкриття злочинів з використанням інформаційних технологій і протидію кіберзлочинності [7].

З урахуванням викладеного матеріалу можна зробити такі висновки. Для ефективної протидії кіберзлочинності відомчих ініціатив уже недостатньо. Потрібна чітка централізована координація зусиль для забезпечення злагодженої взаємодії всіх зацікавлених суб'єктів.

Для поліпшення ситуації необхідно проводити такі заходи:

– сформувати реєстр фахівців з боротьби з кіберзлочинністю з-поміж управлінського апарату, науково-педагогічного складу, практичних працівників, випускників, що пройшли відповідну підготовку;

– за підсумками роботи міжвідомчого науково-практичного заходу, куди необхідно притягнути провідних фахівців, має бути сформована робоча група з удосконалення державної стратегії боротьби з кіберзлочинністю;

– має бути прийняте управлінське рішення про системний розподіл підготовки фахівців з цього напряму в конкретних ВНЗ за конкретними спеціалізаціями для слідчих, оперативних і експертних підрозділів;

– необхідно або усунути дублювання в роботі оперативних підрозділів по боротьбі з кіберзлочинністю, або чітко встановити їх спеціалізацію;

– в ідеалі має бути створене самостійне Центральне Управління по боротьбі з кіберзлочинністю в Україні.

Зважаючи на специфіку діяльності МВС і СБУ, необхідно налагодити взаємодію між ними на етапах підготовки фахівців і проведення наукових досліджень, а в найближчій перспективі – вийти на рівень систематичного проведення спільних оперативно-тактичних навчань.

Боротьба з комп'ютерною злочинністю і кібертероризмом є одним з найважливіших завдань сучасності. Успішність протидії в цьому напрямі багато в чому визначається якістю підготовки фахівців з інформаційної безпеки. Удосконалення навчально-виховної роботи створює передумови для запобігання і попередження комп'ютерної злочинності, особливо, в молодіжному середовищі.

Література:

1. Европейская Конвенция по киберпреступлениям от 23 ноября 2001 г. [Електронний ресурс]. – Режим доступу : http://www.eos.ru.

2. Україна – один з лідерів з кількості кібератак у світі [Електронний ресурс]. – Режим доступу : http://www.pravda.com.ua.

3. Кримінальний кодекс України від 05.01.2001 р. // ВВР України. – 2001. – № 25-26. – Ст. 131.

4. Национальный центр защиты инфраструктур – NIPC [Електронний ресурс]. – Режим доступу : http://www.security-data.ru.

5. Information Assurance Scholarship Program (IASP) [Електронний ресурс]. – Режим доступу : http://www.nsa.gov.

6. *Орлов О. В.* Державне управління підготовкою фахівців у сфері кібербезпеки / О. В. Орлов // Державне будівництво [Електронний ресурс]. – Режим доступу : http://kbuapa.kharkov.ua.

7. Факультет підготовки фахівців для підрозділів по боротьбі з кіберзлочинністю і торгівлею людьми [Електронний ресурс]. – Режим доступу : http://univd.edu.ua.

Надійшла до редколегії 26.03.2014 р.