References

1. *Adepoju, A*. [1994], Preliminary Analysis of Emigration Dynamics in Sub-Saharan Africa. In: *International Migration,* Vol. 32, No. 2, pp. 197-216.

2. *Appleyard, R.T*. [1994], IOM/UNFPA Project on Emigration Dynamics in Developing Countries. In: *International Migration,* Vol. 32, No. 2, pp. 179-195.

3. *Castles, S and M. Miller* [1993], *The Age of Migration: International Population Movements in the Modern World*. Basingstoke, MacMillan.

4. *Massey, D.S.* [1994b], Continuities in Transnational Migration: An Analysis of 19 Mexican Communities. In: *American Journal of Sociology.* (Forthcoming).

5. *Massey, D.S. and F. Garcia-Espana* [1987], The Social Process of International Migration. In: *Science,* Vol. 237, pp. 733-738.

6. *Mullan, B.P.* [1989], The Impact of Social Networks on the Occupational Status of Migrants. In: *International Migration,* Vol. 27, No. 1, pp. 69-86.

7. *Okolski, M.* [1993], *International Migration in Poland: A Country Report.* Manuscript prepared for Workshop on the Causes and Consequences of Emigration from Central and Eastern Europe, Geneva, UN Economic Commission for Europe.

8. *Pyrozhkov, S.I.* [1993], *International Migration in Ukraine: A Country Report.* Manuscript prepared for Workshop on the Causes and Consequences of Emigration from Central and Eastern Europe, Geneva, UN Economic Commission for Europe.

9. *Rogers, R. and E. Copeland* [1993], *Forced Migration, Policy Issues in the Post-Cold War World.* Medford, Mass., The Fletcher School of Law and Diplomacy, Tufts University.

УДК 316.01.0018

Джалладова І. А., д.фіз.-мат.н.,
професор кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет імені Вадима Гетьмана

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: НАУКОВО-ПРИКЛАДНІ АСПЕКТИ І ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ

АНОТАЦІЯ. У роботі наведено аналіз найважливіших проблем сучасності: безпеки інформаційних і комунікаційних систем, захисту від атак за наявності інформаційних війн, розробки при цьому моделі власної поведінки учасника кіберпростору. Показано, що підґрунтям для істотної протидії зростанню злочинів у кіберпросторі може стати грамотна політика національних кадрів у галузі інформаційної безпеки.

КЛЮЧОВІ СЛОВА: інформаційна безпека, ІБ-фахівець, інформаційна війна, кіберпростір, кіберзлочинець, людський фактор, фрод, клятва ІБ-фахівця.

ANNOTATION. This paper presents an analysis of the most important issues of our time: the security of information and communication systems, protection against attacks in the presence of information warfare, while developing its own model of behavior by cyberspace. It is shown that the basis for significant growth combating crime in cyberspace can become competent national personnel policy in the field of information security.

Вступ. Глобальні процеси інформатизації сучасного суспільства і освіти зумовлюють істотне загострення проблем інформаційної безпеки. Інформаційні продукти стають матеріальними цінностями, зростають потреби в їх захисті [1–8]. Інформаційні системи, сервіси телекомунікаційних мереж, електронні платіжні структури вже є невід'ємною частиною життєдіяльності сучасної людини. Інтернет у сучасному світі стає місцем ведення інформаційних війн. У Всесвітній мережі існує велика кількість форумів, блогів і соціальних мереж, у яких користувачі обмінюються інформацією, у зв'язку з цим Інтернет активно використовується для поширення «зараженої інформації».

Нагальним завданням сучасної освіти стає розробка таких методів роботи, в яких гармонійно поєднувалося би навчання сучасним інформаційним технологіям з формуванням високих моральних якостей, для вироблення імунітету до скоєння комп'ютерних злочинів. Така мета поставлена при розробці Концепції підготовки ***ІБ фахівців*** на факультеті інформаційних систем і технологій у Київському національному економічному університеті ім. Вадима Гетьмана.

Одним із найважливіших завдань сьогодення є боротьба з комп'ютерною злочинністю і кібертероризмом. Спектр злочинів у сфері інформаційних технологій, за відомостями системи обліку злочинів Cybersnitch Voluntary Online Crime Reporting System (http://www.cybersnitch.net/csinfo/csdatabase.asp) [19], досить широкий і варіюється від інтернет-шахрайства до дитячої порнографії та включає такі потенційно небезпечні діяння, як електронне шпигунство і підготовка до терористичних актів. Згідно з дослідженнями Meridien (www.epaynews.com/statistics/fraud.html), втрати тільки від інтернет-шахрайства становитимуть у 2015 р. 15–25 млрд дол. США.

Невід'ємною складовою державної політики України, спрямованої на захист інформаційних ресурсів держави та захист інформації з обмеженим доступом, є підготовка фахівців у сфері захисту інформації та інформаційної безпеки. Завдання підготовки фахівців є особливо актуальним ще й тому, що в даний час досить

вільно поширюються друковані видання, в яких описуються технології здійснення комп'ютерних злочинів (наприклад, «Хакер» і «Спецхакер»), які отримали особливу популярність серед молоді. У наш час будь-який підліток може купити за невеликі гроші книгу, яка навчить його елементарним прийомам атаки на інформаційні системи. За допомогою викладених знань такий підліток стає реальною загрозою безпеці комп'ютерних систем. В Інтернеті можна вівшукати майже 30 тисяч сайтів, які навчать комп'ютерному злому [18]. У мережі Інтернет проводяться форуми, віртуальні конференції та семінари з обміну досвідом здійснення комп'ютерних злочинів. Таким чином, комп'ютерні злочинці активно працюють над підвищенням своєї кваліфікації, втягують у своє середовище підростаюче покоління й активно його навчають, причому легально. Все це підкреслює важливість вирішення ще одного завдання — активної протидії залученню молоді до злочинного середовища і розробки ефективних методів проведення виховної роботи серед молоді.

Практика останніх років показує, що підготовка фахівців у галузі інформаційної безпеки стає не тільки актуальною, ***але й життєво необхідною*** для існування підприємства. Ризики для компанії, пов'язані з різними впливами на її інформаційну інфраструктуру, є невід'ємною частиною процесу управління безперервністю бізнесу.

Сутність проблеми

1. Проблема інформаційної безпеки в компаніях. Ідеальний варіант вирішення питань інформаційної безпеки в компанії виглядає таким чином [3]:

• створено й успішно функціонує система управління інформаційною безпекою;

• відпрацьовані всі необхідні документи;

• реалізовані різні сучасні методи та способи захисту інформації;

• функціонує структурний підрозділ, відповідальний за захист інформації;

• всі співробітники усвідомлюють важливість завдання забезпечення інформаційної безпеки і строго дотримуються запропонованих їм інструкцій та регламентів.

Проте в реальності все буває інакше: питання інформаційної безпеки вирішуються за залишковим принципом, документи в галузі інформаційної безпеки розроблені формально і не актуалізуються, а наказ про призначення співробітника на відповідну

посадову позицію видається тільки на виконання вимог регуляторів. Але найбільшою проблемою залишається нерозуміння необхідності вирішувати завдання забезпечення інформаційної безпеки всім колективом підприємства.

2. Проблема інформаційних війн.

Інформаційна війна — це будь-яка атака проти інформаційної функції, незалежно від застосовуваних засобів [17–26].

Припустимо, нам необхідно розмістити в Інтернеті «заражену інформацію». Для цього існує два способи ведення: непрямий і прямий.

За непрямого способу ведення війни потрібно створити інтернет-ресурс або ресурси, на яких буде розміщена необхідна нам інформація. Коли супротивник потрапить на даний ресурс і скористається «зараженою інформацією», атака буде завершена.

За прямого способу ведення війни «заражена інформація» розміщується на ресурсах супротивника або на поширених раніше інформаційних порталах.

Існують ***три мети інформаційної війни***:

1) контролювати інформаційний простір, щоб могли використовувати його, захищаючи при цьому військові інформаційні функції від ворожих дій (контрінформація);

2) контролювати інформацію для ведення інформаційних атак на ворога;

3) підвищити загальну ефективність збройних сил за допомогою повсюдного використання військових інформаційних функцій.

Якщо треба вразити інтернет-ресурс «зараженої інформацією», то спочатку потрібно визначитися з аудиторією. На кожному форумі (блозі, в соціальній мережі і т. п.) існують групи людей, об'єднаних за інтересами. Між такими група часто трапляються розбіжності. Правильно створена і запущена ***інформаційна бомба***, яка враховує особливості ресурсу, викличе бурхливе обговорення. Враховуючи той факт, що спостерігачів набагато більше за учасників баталій, то ефект від атаки може бути колосальним.

Для підвищення якості БОРОТЬБИ і перемоги в інформаційних війнах слід об'єднати професіоналів з інформаційної безпеки у певні асоціації, які б безпосередньо представляли інтереси суспільства споживачів засобів захисту інформації.

В умовах, коли, за оцінками експертів, інформація втрачає актуальність буквально за години, найважливішим напрямом діяльності асоціації буде оперативне інформування ІБ-фахівців про ІБ-загрози, що допоможе їм відображати спрямовані кібер-

атаки і протидіяти вірусним програмним епідеміям. Такі угрупування також можуть слугувати майданчиком, на якому можна отримувати експертну та ***аналітичну інформацію, очищену від маркетингової складової*** і спрощувати практичне застосування документів, що випускаються держорганами в галузі стандартизації та регулювання ІБ. Це допоможе ІБ-керівникам вибудовувати стратегію своєї роботи.

Констатуючи в суспільстві низьку культуру використання ІТ з позицій ІБ, асоціація повинна взяти на себе зобов'язання розробляти практичні регламенти по ІБ для пересічних ІТ-користувачів. Це допоможе людям освоїти основні прийоми «***інформаційного самозахисту***» і допомагати державі ***захищати громадян від небажаної та негативної інформації*** як на практичному рівні, так і в розробці стратегії цього напряму.

Виникненню експертних спільнот професіоналів сприяють і сучасні засоби комунікацій. Вони відіграють важливу роль не тільки з позиції обміну досвідом, а й формують певний міжнародний інтелект.

Створення великих експертних мережевих спільнот професіоналів спроможне брати участь в оцінках важливих суспільних явищ, допомагати урядам, політикам, бізнес-керівникам різного рівня приймати рішення із найважливіших завдань. Адже кваліфіковано оцінювати різні явища і події в суспільстві можуть лише фахівці. До того ж актуальним залишається створення спільних міжнародних асоціацій ІБ фахівців.

3. Проблема інформаційної безпеки — одна з найактуальніших на сьогоднішній день. XXI століття є століттям інформації, нових інформаційних технологій. Інформатизація та телекомунікації є ланцюгом інфраструктури, який з'єднує сьогодні всі галузі економіки в єдине ціле. З іншого боку, до інформації значно підвищується інтерес кримінальних структур, організацій, що займаються недобросовісною конкуренцією. За даними МВС, останнім часом ОБСЯГ кіберзлочинів у державі зріс у 150 разів, при тому що латентність злочинності в цій сфері сягає 90 %.

Захищати інформацію обов'язково потрібно, а для телекомунікаційних компаній це завдання є першочерговим. Доступність і цілісність переданої по мережах інформації прямо пов'язані з доходами оператора зв'язку, а їх порушення призводить до фінансових збитків, втрати іміджу і клієнтів.

На сьогодні серйозною проблемою стало шахрайство в мережах зв'язку, так званий ***фрод***: незаконні переговорні пункти, несанкціоновані підключення до каналів зв'язку, шахрайство в бі-

лінгових системах, підробка засобів платежів за послуги зв'язку. Всі ці проблеми вимагають адекватної відповіді — наявності високопрофесійних, підготовлених фахівців. До того ж істотно зросла інтенсивність ураження мережі Інтернет шкідливим контентом, так званими *вірусами*, *хробаками*, *троянськими кіньми*, які виводять з ладу значну кількість серверів. Наслідком цього є і помітне збільшення навантаження на комутаційне обладнання за обсягом переданої інформації. «Віруси» знищують інформацію на жорстких дисках, вносять зміни до реєстрів, викликають переповнення буферів і порушують працездатність комутаційного обладнання.

Комп'ютерні злочини є одним із способів ведення інформаційної війни з метою ідеологічного та психологічного впливу на свідомість окремого індивіда, соціальних груп, розпалювання етнічної та релігійної ворожнечі. Тому фахівець із захисту інформації зобов'язаний знати стратегію і тактику ведення інформаційної війни, вражаючі фактори інформаційної зброї і прийоми протидії інформаційним операціям.

Вплив інформації на людину

Встановлено, що інтенсивний інформаційний вплив викликає змінений стан свідомості [3, 4]. Відбувається зміна статусу особистості (людина неадекватно оцінює себе і свої можливості) і статусу свідомості. Змінений стан свідомості обумовлює трансформації сприйняття (зрушення порогів, синестезії), зміни емоційного тону відчуттів і структури афектів, пам'яті (спонтанні вилучення з пам'яті давно пережитих ситуацій, іноді переходять у регресію поведінки), зміна сприйняття плину часу (уповільнення, прискорення, роздроблення). Тут важливо підкреслити, що змінені стани свідомості стимулюють розвиток регресії поведінки, яка трактується психологами як специфічна форма втечі індивіда від дійсності, тимчасове повернення його на ранню стадію розвитку, до примітивніших форм поведінки і мислення.

Дослідження дозволяють стверджувати, що накопичення деструктивної інформації в підсвідомості має кумулятивний характер (підсумовування негативного ефекту при кожному впливі). В організмі йде накопичення свого роду інформаційного токсину до деякого критичного значення. У момент переходу (в точці біфуркації) і виникають деструктивні стани в організмі. З одного боку, вони стимулюють виникнення серйозних соматичних захворювань (аж до онкологічних), можуть змінити структуру ДНК людини, приводячи до необоротних генетичним наслідків. З дру-

гого — сприяють деструкції особистості, зміні світогляду людини, формування неадекватного сприйняття дійсності. Найчастіше такий стан залишається неусвідомленим. Однак це може стати причиною значних катастроф, викликаних придушенням професійних навичок у роботі на відповідальних ділянках (диспетчер управління руху в аеропортах, оператор атомних електростанцій тощо). Аналогічна небезпека може виникнути у фахівців в інших сферах. Саме страх пригнічує професійні якості і не дає можливості адекватно і швидко реагувати на мінливість ситуації.

Особливу небезпеку становить протиправне застосування спеціальних засобів впливу на індивідуальну, групову та суспільну свідомість [23–26]. При цьому метою є девальвація духовних цінностей і пропаганда зразків масової культури, заснованих на культі насильства, на духовних і моральних цінностях, що суперечать цінностям, прийнятим у суспільстві. Зниження духовного, морального і творчого потенціалу населення помітно ускладнює підготовку трудових ресурсів для впровадження і використання новітніх технологій, у тому числі інформаційних.

Історичний огляд підготовки фахівців з інформаційної безпеки

Питання підготовки, перепідготовки та підвищення кваліфікації фахівців з інформаційної безпеки (ІБ) в Україні вперше було поставлено в другій половині 1960-х років.

Тоді він розглядався тільки в площині кадрового забезпечення захисту державних секретів, оскільки комерційної таємниці в СРСР не існувало, а захист несекретної інформації не був актуальним, як сьогодні.

З початку 1990-х років з'явились нові фактори, які вплинули на підготовку та підвищення кваліфікації фахівців з ІБ, найважливіші з яких такі:

— розширення інформаційної галузі;

— розширення обсягу інформації, що підлягає захисту;

— ускладнення умов зберігання та захисту інформації.

Хоча обсяг державних секретів України порівняно з СРСР знизився, але він продовжує залишатися значним у найважливіших сферах діяльності держави. Про це свідчать Закони України «Про інформацію», «Про державну таємницю» та інші нормативні документи.

Обсяг інформації, що захищається, не скоротиться, оскільки в Україні з огляду на її геополітичне становище, військовий та економічний потенціал зберігається велика кількість інформації

про політичні, військові, економічні, науково-технічні та інші сектори держави. Така інформація потребує надійного захисту, оскільки її витік здатний викликати політичні ускладнення, ослаблення військової та економічної потужності країни.

Однак поряд із продовженням існування державної таємниці з'явилася і комерційна таємниця. Від надійності захисту цієї інформації залежить ефективність функціонування комерційних підприємств, їх безпека та конкурентоспроможність.

Не випадково, що при створенні спільних підприємств вимога до захисту комерційної таємниці висувається зарубіжними партнерами як одна з ключових. У надійному забезпеченні захисту комерційної таємниці зацікавлена і держава, враховуючи пряму залежність економічного становища країни від стану економіки на підприємствах недержавного сектору.

Компетентний фахівець зобов'язаний стати еталоном суб'єкта безпечної інформаційної діяльності і при цьому знатися на питаннях інформаційної безпеки в усіх аспектах: юридичних, психологічних, соціально-історичних, педагогічних, програмно-технічних. Адже інформація (інформаційні ресурси, цінності) та її інфраструктура — це та основа, з якою їм доведеться працювати і жити в XXI столітті.

Становлення наукового напряму «Інформаційна безпека» в Україні

Становлення наукового напряму «Інформаційна безпека та захист інформації» в Україні пов'язано з іменами таких *видатних учених*, як О. М. Новіков, О. К. Юдін, Г. Ф. Конахович, О. Г. Корченко, І. Д. Горбенко, В. В. Поповський, В. Б. Дудикевич, Є. А. Мачутській, В. М. Шокало, В. В. Домарєв, В. А. Шокало та ін.

Поточний стан проблеми інформаційної безпеки з педагогічної точки зору при аналізі показує її недостатню розробленість, оскільки різні аспекти інформаційної безпеки знаходять поки відображення здебільшого в правознавстві, технічних і природничих науках, в політології та соціології. З урахуванням проблем, які викладено у вступі даної роботи, курс «Інформаційна безпека» треба викладати зі школи (електронні засоби навчання для інтерактивної дошки за темами інформаційної безпеки) і мережевий портал «Криптоленд» на http://lomasko.com можуть використовуватися в практиці підготовки). У дисципліні «Інформаційна безпека» необхідно відобразити такі розділи: основні підходи до забезпечення інформаційної безпеки; інформаційна етика та інформаційне право; світова і вітчизняна історія захисту інформа-

ції; криптологія та захист інформації; сучасні засоби і технології захисту інформації.

Концептуальну основу підготовки в галузі інформаційної безпеки складають нормативно-правові документи, прийняті в Україні. Перш за все — в Концепції Національної безпеки України [5] як однієї із загроз національній безпеці держави в науково-технічній сфері вказувалося: «зниження рівня підготовки висококваліфікованих наукових та інженерно-технічних кадрів»; у постанові Кабінету міністрів України від 08.10.1997 № 1126 «Про затвердження Концепції технічного захисту інформації в Україні» [13] увага акцентується на тому, що одним з основних напрямів державної політики у сфері технічного захисту інформації є підготовка кадрів у сфері технічних систем захисту інформації.

З метою створення повноцінної та ефективної системи підготовки кадрів у напрямі інформаційної безпеки починаючи з 1995 року, коли був підписаний спільний наказ Державної служби України з питань технічного захисту інформації та Міністерства освіти України від 28.12.1995 № 66/358 «Про співробітництво між Міністерством освіти Україна та Державною службою України з питань технічного захисту інформації». Згідно з цим наказом у ряді міст України (Київ, Харків, Одеса, Львів, Миколаїв, Дніпропетровськ та ін.) розпочалася підготовка фахівців із захисту інформації.

Аналіз навчальних планів і програм підготовки фахівців в сфері захисту інформації, стану наукової та навчально-педагогічної діяльності дозволяє виділити навчальні заклади, в яких найбільш якісно готуються фахівці: Національний технічний університет України (НТУУ) «КПІ», Київський міжнародний університет цивільної авіації (КМУЦА), Державний університет інформаційно-комунікаційних технологій (ДУІКТ), Харківський державний технічний університет радіоелектроніки та ін.

Актуальність підготовки ІБ фахівців у КНЕУ на ФІСІТ

Під час підготовки до 50-річного ювілею факультету інформаційних систем і технологій КНЕУ на міжкафедральному семінарі виступив професор О. Д. Шарапов. Тема доповіді стосувалася науково-прикладних аспектів ІТ технологій і систем та існуючих проблем, пов’язаних з інформаційною безпекою, а також проблеми підготовки висококваліфікованих кадрів у галузі ІБ на факультеті ФІСІТ у КНЕУ.

Доповідь професора О. Д. Шарапова було добре структурована. Доповідач показав гарне володіння предметом і наявність чи-

малого практичного досвіду у вирішенні різних завдань, пов'язаних з інформаційними технологіями, у тому числі і питаннями інформаційної безпеки. Фактично обговорювалися всі основні аспекти ІБ: понятійні основи, нормативна база та міжнародні стандарти, види сучасних загроз, питання аналізу ПО, застосування методів криптографії в автоматизованих системах, довірені платформи і довірена базове ПЗ і їх сертифікація, номенклатура необхідних спеціальностей в сфері ІБ, приблизний обсяг знань для спеціальностей з ІБ і багато іншого.

На закінчення доповідач приділив увагу тому, що, незважаючи на актуальність підготовки високопрофесійних кадрів в сфері ІБ і наявність необхідного на ФІСІТ потенціалу, однак на факультеті не ліцензована відповідна спеціальність і не ведеться підготовка таких фахівців.

Була висловлена думка під час обговорення доповіді, що аналіз стандарту за фахом 6.170101 «Безпека інформаційних систем …» передбачає випуск спеціалістів із відповідною профільною підготовкою в сфері ІБ і відповідає ***духу кафедри комп'ютерної математики та інформаційної безпеки, що тяжіє до посиленої математичної підготовки і інформаційної культури***. Тому реалізація даної або близькою до неї спеціальності на факультеті зі змістовної позиції не буде проблематичною.

Для повноцінної підготовки фахівців з ІБ на факультеті є і відповідне матеріально-технічне забезпечення з відповідними класами та бібліотекою.

Керівництво університету дало позитивну оцінку як доповіді, так і висновкам про важливість розгортання в КНЕУ відповідної навчальної діяльності з підготовки фахівців з інформаційної безпеки. У зв'язку з чим поява на факультеті нової спеціальності стала вельми реальною. Відповідальною за підготовку цієї спеціальності стала кафедра комп'ютерної математики та інформаційної безпеки.

Основні напрями удосконалення підготовки фахівців у галузі інформаційної безпеки в КНЕУ

Проблема вдосконалення підготовки фахівців у галузі інформаційної безпеки є багатоплановою. Для вироблення рекомендацій щодо вдосконалення підготовки фахівців у галузі інформаційної безпеки умовно *виділимо три напрями, в межах яких пропонується здійснити оптимізацію діяльності учасників навчального процесу: навчально-виховне, навчально-методичне, організаційно-адміністративний.*

1. Однією з важливих умов підвищення якості підготовки фахівців у галузі інформаційної безпеки є формування високих моральних якостей у студентів. Недостатня увага до людського фактора, як правило, є значнішою загрозою, ніж використання новітніх технічних засобів для здобуття конфіденційної інформації. Під *поняттям «людський фактор»* психологи розуміють «сукупність властивостей людини оператора, що впливають на ефективність системи «людина — машина» [8].

Пропонується за доцільне розширити визначення: це інтегральна характеристика особистості, що визначає надійність захисту інформації при її отриманні, зберіганні та переробці в автоматизованих техніко-біологічних системах. *Незважаючи на різноманітність і постійне вдосконалення спеціальної техніки для захисту інформації, люди залишаються найслабшою ланкою в людино-машинних системах, одним з найвірогідніших джерел витоку інформації.*

Тому вважається за потрібне на факультеті створювати спеціальну лабораторію, яка могла б займатися вивченням мотивації студентів до скоєння протиправних дій у галузі інформаційних технологій і виробленням рекомендацій для оперативного коригування навчально-виховної роботи серед молоді.

Одним із головних напрямів діяльності таких підрозділів має бути проведення профорієнтаційної роботи серед молоді та обов'язкового тестування абітурієнтів на їх професійну придатність. Такий напрям успішно розвивається в США. На думку Д. Л. Шіндера [8], одним із способів скорочення кількості кіберзлочинів є використання впливу лідерів соціальних груп. Як показали соціологічні дослідження, проведені в США, вплив авторитетів у соціальних групах діє на поведінку людей. Так, зниження кількості курців у США в значній мірі пов'язане з соціальним клеймом курця.

Таким чином, одним з важливих чинників підвищення якості підготовки фахівців у галузі інформаційної безпеки мають бути заходи з посилення режиму відбору на спеціальності, пов'язані із захистом інформаційних технологій.

На факультеті ІСіТ навчально-виховна робота повинна бути поставлена таким чином, щоб активно залучити фахівців з комп'ютерних технологій у боротьбу з кіберзлочинністю, або хоча б ізолювати їх від злочинного середовища. Планується в курсі «Вступ в інформаційну безпеку» викладати розділ «Кодекс комп'ютерної етики», спираючись на те, що повага до власності інших осіб у віртуальному світі настільки ж важлива, як у світі фі-

зичному. Звичайно, є ті, хто вчинить злочин незалежно від громадської думки, але вплив авторитету — цінний інструмент проти багатьох правопорушень, скоєних тільки через помилкову віру в те, що «всі це роблять». В ідеалі необхідно, щоб фахівці з інформаційної безпеки символічно давали «Клятву ІТ-, ІБ-фахівця».

2. Концепція програми підготовки на кафедрі КМІБ передбачає вирішення таких завдань: формування правової культури в галузі інформаційних технологій, коригування існуючих навчальних програм, запровадження нових навчальних дисциплін. Для відображення сучасних досягнень у галузі захисту інформації планується регулярно (не менше 1 разу на рік) переглядати зміст спеціальних навчальних дисциплін. У даний час у навчальні програми підготовки фахівців у галузі інформаційної безпеки введено дисципліни з ***нормативно-правової бази інформаційних технологій і стратегії і тактики інформаційної війни***.

Зокрема, введена дисципліна «Правознавство» (назва умовна). Мета вивчення дисципліни: ознайомити студентів з правовими аспектами експлуатації обчислювальної техніки, показати невідворотність покарання за вчинення комп'ютерних злочинів. У процесі вивчення дисципліни студенти повинні ознайомиться з основними положеннями Законів України «Про авторське право і суміжні права», «Про інформацію» та розділом 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» Кримінального кодексу Україна.

До навчального плану підготовки фахівців із захисту інформації введена дисципліна «Інформаційна культура», одним із модулів якої пропонується тема «Розслідування комп'ютерних інцидентів», метою якої є ознайомлення студентів із використовуваними правоохоронними органами методами запобігання та припинення спроб неправомірного доступу до комп'ютерної інформації, що становить комерційну (службову) таємницю, а також існуючими підходами до розслідування комп'ютерних злочинів.

Вважається доцільного у навчальному плані підготовки фахівців у галузі інформаційної безпеки наявність дисципліни «***Захист інформації у біологічних системах***». У дисципліні пропонується вивчення таких питань:

1. Інформатизація суспільства і проблема захисту інформації (ретроспективний аналіз підходів до формування безлічі загроз інформації; інформаційна війна: методологічні основи; модель і принципи інформаційної війни; інформаційний простір і громадська думка, як об'єкт впливу).

2. Правові основи інформаційної безпеки (правове забезпечення інформаційної безпеки з захисту прав та інтересів особи, суспільства і держави; визначення і зміст поняття загрози інформації в сучасних системах її обробки; концепція національної безпеки України; нормативно-правові акти України; поняття про інформаційну безпеку людини, суспільства, держави).

3. Захист інформації в біологічних системах (інформаційна війна як цілеспрямований інформаційний вплив інформаційних систем на людину; прийоми інформаційного впливу; загальні принципи захисту інформації в біологічних системах).

Огляд підходів підготовки фахівців з інформаційної безпеки в США та країнах Європи

У США найсерйознішу увагу приділяють проблемі підготовки фахівців для захисту національних інформаційних структур. Важливо зазначити, що в США дуже багато уваги приділяється залученню суспільної уваги до проблеми інформаційної безпеки (http://www.staysafeonline.info). Міжнародна асоціація фахівців з комп'ютерних досліджень (IACIS) забезпечує навчання в галузі комп'ютерних технологій (http://www.nips.gov). Успішно функціонує Національна спілка кібербезпеки, яку створено спільно урядом і промисловцями США. Мета спілки — розробка підходів до проблеми безпеки в кіберпросторі, підвищення рівня освіти в сфері інформаційної безпеки, залучення суспільної уваги до проблеми кібертероризму [2].

Проведений огляд інтернет-сайтів, присвячених підготовці фахівців у США, дозволив виділити найбільші компанії, що проводять навчання в галузі інформаційної безпеки: Check Point Software Technologies, Cisco Systems, IBM Tivoli Systems Global Security Laboratory, Internet Security Systems, Microsoft, Network Associates, Prosoft Training. Com, Sun Microsystems, Symantec. Серед навчальних центрів, що спеціалізуються на підготовці фахівців із захисту інформації, можна відзначити: CERT, GIAC, CSI, Cisco Systems.

Крім комерційних компаній, підготовку фахівців у галузі інформаційної безпеки здійснює ряд державних структур. Для вдосконалення методів навчання в Міністерстві оборони створено спеціальний підрозділ — «Управління програм з інформаційної безпеки (Information Assurance Program Office)». Агентство національної безпеки (NSA) сформувало ще в 1999 р. низку центрів післявузівської освіти, а в 2000 р. підключило до них 14 провідних університетів США. Одночасно Білий Дім розпочав навчання урядовців (до 10 тис. осіб) у рамках федеральної програми забезпечення безпеки інформаційних технологій з бюджетом 25 млн дол. на рік [4].

Одним із напрямів удосконалення системи підготовки фахівців із захисту інформації у США бачать у створенні міжнародних консорціумів.

Інтернаціональний характер проблеми державного забезпечення захисту інформації вимагає консолідації та координації зусиль усіх країн у плані підготовки фахівців із захисту інформації. США виступили ініціаторами створення мережі міжнародних консорціумів з підготовки кадрів у галузі захисту інформації.

Світовим лідером із сертифікації фахівців з інформаційної безпеки є міжнародний консорціум з сертифікації в галузі безпеки інформаційних систем: International Information Systems Security Certification Consortium, Inc. — (ISC) 2, який базується у Відні і Вірджинії, а також має офіси в Лондоні та Гонконгу (http://www.isc2.org/). (ISC) 2 є головною організацією в забезпеченні професіоналів у галузі інформаційної безпеки та фахівців-практиків усього світу стандартом професійної сертифікації, заснованому на загальноприйнятому обсязі знань (ISC) 2 для фахівців з інформаційної безпеки. Існуючи понад 14 років, (ISC) 2 уже сертифікував тисячі професіоналів з безпеки із 100 країн.

До претендентів на отримання сертифіката Certified Information Systems Security Professional (CISSP) висувають досить високі вимоги. Необхідно мати досвід не менше як чотири роки роботи спеціалістом з інформаційного захисту (або не менше як три роки і ступінь бакалавра), здати складний іспит, підписати Кодекс етики (ISC) 2 і постійно підтримувати свою кваліфікацію. Для підтвердження сертифікації CISSP не вимагається повторної здачі іспиту, досить кожні три роки проходити навчання на авторизованих курсах з інформаційної безпеки і брати участь у конференціях з цієї теми.

Питання підготовки охоплюють широкий діапазон проблем безпеки, заснованих на загальноприйнятому обсязі знань (Common Body of Knowledge, CBK). CBK складається з десяти доменів: методи управління інформаційною безпекою, архітектура і моделі безпеки, методологія і системи управління доступом, безпека розробки додатків і систем, безпека операцій, фізична безпека, криптографія, безпека телекомунікацій, мереж та Інтернет, планування безперервності бізнесу та планування відновлення після збоїв, законодавство, розслідування та етика.

З метою налагодження партнерських зв'язків з навчальними закладами Європи, Близького Сходу і Африки співробітники Стенфордського університету в 1984 р. створили фірму Cisco Systems. Був створений освітній проект «Мережева академія

Cisco», який здійснюється спільно освітніми установами і компанією Cisco — світовим лідером у галузі мережевих інтернет-рішень. На початку своєї діяльності академія планувалася для підготовки кваліфікованих кадрів з обслуговування мереж, проте надалі набула популярності як потужний центр підготовки фахівців із захисту інформації.

У даний час мережева академія Cisco є світовим лідером у мережних технологіях для Інтернет і забезпечує фундаментальну підготовку фахівців з теорії та практики проектування, будівництва та технічного супроводу локальних і глобальних мереж із використанням загальновизнаних стандартів і рішень в галузі інформаційної безпеки.

Академії Cisco відкриті в 152 країнах (всього у світі понад 10 тис. академій), у яких навчається понад 470 тис. студентів. Станом на квітень 2004 р. мережевих академії: у Росії — 33, в Україні — 17 (для порівняння — у Великобританії — 565, в Італії — 320, у Німеччині — 291). Навчання проводиться дев'ятьма мовами. Навчальний матеріал оновлюється кожні 90 днів.

Слід зауважити, що детальніше вивчення навчальних програм ділового адміністрування показує, що в них знаходять серйозний розгляд питання інформаційної безпеки, а також питання, пов'язані з вивченням легальних методів отримання інформації про конкурентів (*конкурентна розвідка*).

Соціологічні дослідження

Аналізуючи ситуацію з підготовкою кадрів, цікаво навести результати соціологічних досліджень серед молоді, яка планує займатись IT безпекою у майбутньому.

Здійснення комп'ютерних правопорушень у молоді викликає захоплення, бажання самоствердитися, показати себе з кращого боку і привернути увагу. Дійсно, часто хакери здійснюють зломи мережі, щоб справити враження на оточення. Серед інших факторів, що визначають бажання здійснювати комп'ютерні правопорушення, можна виділити бажання заробити.

Багато абітурієнтів, вступаючи на спеціальності, пов'язаної із захистом інформації, переслідують корисливу мету — навчитися методам здійснення комп'ютерних злочинів.

Переважна більшість студентів, що навчаються на спеціальностях, пов'язаних з обчислювальною технікою, слабо знають нормативно-правові документи з захисту інформації, зокрема, вони практично не знають, яку відповідальність несе зловмисник за скоєння комп'ютерних злочинів.

У даний час актуальним завданням втрачається розробка методичних засад для ефективної роботи із запобігання комп'ютерних злочинів, формування нетерплячості до протиправних дій у галузі інформаційних технологій. У зв'язку з цим цікавим є ознайомлення із результатами соціологічних опитувань (тестів), спрямованих на виявлення мотивації фахівців до скоєння протиправних дій у галузі авторського права та комп'ютерних злочинів, визначення їх рівня правової грамотності в галузі захисту інтелектуальної власності та їх ставлення до порушників інформаційної безпеки.

У тестах є питання, які дозволяють з'ясувати у респондентів:

• ставлення до поняття «хакер»;

• ставлення до матеріалів (інтернет-сайти, література), присвячених питанням злому захисту інформації;

• бажання і мотиви вивчення технологій здійснення комп'ютерних злочинів (написання вірус-програм та інших шкідливих програм, злому комп'ютерів і мереж, злому захисту банківської системи, підробки кредитних карток, безкоштовному доступу до інтернет-ресурсів і міжміської телефонної мережі);

• рівень знання юридичних нормативних документів щодо захисту інформації (Законів України «Про авторське право і суміжні права», «Про інформацію», розділом 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж» Кримінального кодексу України) [12–15, 23].

За допомогою тестування з'ясували ставлення респондентів до поняття «хакер». Цікаво, що респонденти, діяльність яких буде пов'язана з експлуатацією, суворіше ставляться до протиправних діянь хакера (у середньому 37 % опитуваних вважають дії хакера злочинними). Респонденти спеціальностей, пов'язаних із захистом інформації, лояльніше ставляться до дій хакера. Додаткові дослідження показали, що для них хакер — насамперед фахівець найвищої кваліфікації, який часто виступає як борець за справедливість і гідний наслідування.

Далі дослідження зосередили в основному на студентах спеціальностей, пов'язаних із захистом інформації. Зокрема, визначили мотиви вступу до навчальних закладів за обраною спеціальністю і виявили пріоритети у вивченні спеціальних дисциплін. Слід зазначити, що 38 % опитуваних вважають за потрібне використовувати знання технології хакерських атак для побудови ефективного захисту, 17 % студентів бажають вивчати методи здійснення комп'ютерних злочинів з метою заробітку на зломі інформації, 13 % опитуваних допускають можливість здійснення протиправних діянь при необхідності помститися кривднику. Можна припустити, що в да-

ному випадку діагностується мала інформованість респондентів про відповідальність за вчинення комп'ютерних злочинів.

Мета проведених досліджень — показати можливі тенденції формування мотивів тієї частини молоді, діяльність який пов'язана з інформаційними технологіями і звернути увагу на необхідність продовження досліджень у цьому напрямі для виявлення прихованої злочинності та розробки ефективних заходів із запобігання злочинів у сфері високих технологій.

Таким чином, можна констатувати, що сучасний підхід до організації підготовки ІБ-фахівців ще треба удосконалювати, з метою запобігання кіберзлочинності і перемоги у інформаційній війні, і тому діяльність ФІСІТ з відкриття спеціальності «Безпека інформаційних і комунікаційних систем» на часі.

Висновки. Кіберзлочинність сьогодні — це багатомільярдна індустрія [21–26]. Успішність протидії їй багато в чому визначається якістю підготовки фахівців з інформаційної безпеки. Удосконалення навчальних програм підготовки ІБ фахівців створює передумови для запобігання та попередження комп'ютерної злочинності, особливо в молодіжному середовищі.

Попри існуючу систему підготовки та перепідготовки фахівців в Україні і у зв'язку з вимогами часу наочним є постійне її вдосконалення. У даній статті було зроблено спробу комплексно розглянути проблеми підготовки кадрів в Україні як в галузі технічних питань захисту інформації, так і в сфері боротьби з комп'ютерною злочинністю, включаючи питання формування правової грамотності із запобігання комп'ютерних злочинів студентів технічних, в першу чергу — комп'ютерних спеціальностей.

Процес навчання фахівців у галузі інформаційної безпеки умовно можна розділити на підготовку керівників і співробітників, відповідальних за цю діяльність у компанії. Усе це повинно відбуватися на тлі підвищення обізнаності кожного співробітника компанії в питаннях інформаційної безпеки. Рядові співробітники, як правило, про інформаційну безпеку мають віддалене уявлення, а їх обізнаність обмежується епізодичними нагадуваннями керівництва про необхідність суворо дотримуватись розпоряджень, різних інструкцій і регламентів. При цьому така діяльність, як правило, активізується, коли в компанії вже щось сталося. У цьому разі потрібні не просто фахівці з інформаційної безпеки, а експерти, здатні здійснювати весь комплекс заходів у даній царині, включаючи відповідну підготовку рядових працівників. Взагалі фахівець у галузі інформаційної безпеки повинен підвищувати свою кваліфікацію як мінімум щорічно, тому що постійно виникають нові і нові

загрози саме через високу технологічність цієї галузі діяльності. З'являються усе нові версії операційних систем, а в них — нові сервіси, служби, можливості. Загальна тенденція міграції мереж зв'язку в мережі передачі даних, тобто комп'ютеризація мереж зв'язку, призводить до того, що загрози безпеки стають усе більш і більш технологічно складними.

На кафедрі комп'ютерної математики та інформаційної безпеки враховуються такі напрями діяльності:

1) спрямованість навчання на поглиблену теоретичну підготовку фахівців за найзагальнішими аспектам безпеки і ознайомлення з відносно повним спектром методів і систем захисту інформації;

2) акцент на практичну спрямованість навчання (у межах навчальних програм велика увага приділяється лабораторним роботам і практичним заняттям);

3) орієнтація на вивчення конкретних продуктів і правил їх експлуатації;

5) висока мобільність змісту курсів, що читаються (швидка реакція на нові технології захисту інформації);

6) проведення навчальних курсів з нормативно-правовій базі захисту інформації;

7) тісні контакти із західними провідними центрами.

Література

1. *Бачило И.Л.* Информационное право. / И. Л. Бачило. — М. : Высшее образование; Юрайт-Издат, 2009. — 321 с.

2. *Венбо, Мао*. Современная криптография: теория и практика / М. Венбо. — М. : Вильямс, 2005. — 768 с.

3. *Вильям Столлингс*. Криптография и защита сетей: принципы и практика / *Вильям Столлингс*. — М. : Вильямс, 2001. — 451 с.

4. *Воронина Т.П.* Информационное общество: сущность, черты, проблемы / Т. П. Воронина. —М., 1995. — 111 с.

5. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — М., 2001.

6. ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи па базе асиметричного криптографического алгоритма. — М., 1995.

7. *Ефремов А*. Информация как объект гражданских прав [Електронний ресурс]. — Режим доступу : hltp://ww\v.russianla\v,nel/ia. — Заголовок з екрану.

8. *Жельников В*. Криптография от папируса до компьютера / В. Жельников. — М. : АВР, 1996. — 211 с.

9. *Конхейм А. Г.* Основы криптографии / А. Г. Конфейм. — М. : Радио и связь, 1987. — 147 с.

10. *Петренко С.А.* Политики информационной безопасности / С. А. Петренко, В. А. Курбатов. — М. : Компания АйТи, 2006. — 400 с.

11. *Рубинштейн С.Л.* Принципы и пути развития психологии / С. Л. Рубинштейн. — М. : L956. — 342 с.

12. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации : руководящий документ [Електронний ресурс]. — Режим доступу : hllp.V/www.fsLec.ru. — Заголовок з екрану.

13. *Алешенков М.* Секьюритология (наука о сохранении и защите ноосферы и человечества) [Електронний ресурс] / М. Алешенков, Б. Родионов. — Режим доступу : hUp://articlcs.cxcelion.iTi.

14. *Шпайер Брюс*. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. — М. :Триумф, 2002. — 467 с.

15. *Мэйволд Эрнст*. Безопасность сетей / Э. Мэйволд. — М. : Эком, 2006. — 347 с.

16. *Ярочкин В.И*. Информационная безопасность : учебник для вузов / В. И. Ярочкин. — М. : Фонд «Мир»: Акад. проект, 2003. — 639 с.

17. *Ящепко В.В*. Введение в криптографию ; под общ. ред. В. В. Ящепко. — СПб. : Питер, 2001.

18. *Горбенко І.Д.* Прикладна криптографія / І. Д. Горбенко. — Харьков, 2001.

19. *Боровко Р*. Более 30 тысяч сайтов обучают компьютерному взлому [Електронний ресурс] / Р. Боровко. — Режим доступу : http://www.cnews.ru/lib/.

20. *Гриняев С*. США развертывают систему информационной безопасности. В России же дальше разговоров дело пока не идет [Електронний ресурс] // Независимое военное обозрение. — № 45 (405). — Режим доступу :http://www.cnews.ru.

21. Кибертерроризм. Обзор [Електронний ресурс]. — Режим доступу : http:// www.crime-research.ru. — 18.08.2004.

22. *Белов Е.Б.* О государственном мониторинге качества образования специалистов по защите информации / Е. Б. Белов // Проблемы информационной безопасности. Компьютерные системы. — 1999. — № 1.

23. Концепція (основи державної політики) Національної безпеки України : Схвалена Постановою Верховної Ради України від 16 січня 1997 р. № 3/97-ВР.

24. Про затвердження Концепції технічного захисту інформації в Україні : Постанова КМ України від 08.10.1997 № 1126.

25. Підготовка фахівців із захисту інформації в Україні / Бабак В.П., Козловський В.В., Хорошко В.О., Чирков Д.В. // Захист інформації. — 2001. — № 4. — С. 57-69.

26. *Шиндер Д.Л.* Киберпреступность [Електронний ресурс] / Шиндер Д.Л. ; [пер. Тропиной Т.]. — Режим доступу : Crime.vl.ru.