НАУКОВИЙ ЖУРНАЛ

ПІВДЕННОУКРАЇНСЬКИЙ ПРАВНИЧИЙ ЧАСОПИС

№ 2

2011

Зареєстровано Державним комітетом телебачення і радіомовлення України
Свідоцтво про державну реєстрацію друкованого засобу масової інформації: Серія КВ № 15252-3824Р від 22.06.2009 р.
Виходить з 1997 р. До 2006 р. - "Вісник Одеського інституту внутрішніх справ". Щоквартальник

Засновник:
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ЗМІСТ

В інших випадках це робить лікар, або ж він допомагає це зробити (наприклад, Голландія). Такий лікар офіційно визначається як уповноважений лікар.

Є ще одна форма здійснення такого процесу, що існує в Італії. Законодавчого закріплення дозволу на евтаназію немає, тому суди "офіційного" дозволу на евтаназію також не дають. Вони "тільки" дозволяють виконати бажання пацієнта або його близьких про припинення лікування або примусового харчування, як у випадку з Елуаною Енглара, яка більше ніж 17 років перебувала в комі (вегетативному стані). Хоча й тут є складнощі між прийняттям відповідного судового рішення і його практичним виконанням. Наприклад, в останньому випадку між первинним рішенням суду та його підтвердженням апеляційним і вищим судами Італії пройшло 9 років з тих 17 років, протягом яких ця пацієнтка була в комі[5, 47].

Тому, незважаючи на законодавчу заборону, виходячи з принципу гуманізму і людського співчуття, уявляється можливим підтримати висловлену точку зору про те, що умисне заподіяння смерті невиліковно хворому пацієнту, учинене медичним працівником на його попереднє прохання, необхідно законодавчо закріпити у вигляді привілейованого складу вбивства.

Причини такого посилення кримінальної відповідальності медичних працівників очевидні. Так якщо медичний працівник, виконуючи неналежним чином свої професійні обов'язки, заподіює з необережності шкоду життю чи здоров'ю пацієнта, то дана обставина є обтяжуючою кримінальну відповідальність у відповідних складах. Водночас, якщо медичний працівник, усупереч своїм професійним обов'язкам, навмисне заподіює смерть або шкоду здоров'ю пацієнта, то для кримінально-правової оцінки цей факт залишається не важливим. Сам факт учинення вбивства, умисного заподіяння тяжкої або середньої тяжкості шкоди здоров'ю пацієнта спеціальним суб'єктом - медичним працівником - покликаним рятувати життя і здоров'я, повинен обтяжувати його кримінальну відповідальність у формально-юридичному плані (за винятком учинення вбивства з мотивів співчуття) [4, 16].

Отже, підсумовуючи, слід зазначити, що зайва криміналізація медичної діяльності, пов'язана з уведенням у кримінальне законодавство нових норм і складів злочинів, пов'язаних з медициною, не завжди виправдана. Доцільно розглядати питання про недопущення невиконання або неналежного виконання своїх професійних обов'язків у різноманітних сферах надання медичної допомоги як професійним медиком, так і особою, яка працює в медичній сфері, з метою формування суспільних відносин у потрібному для всього суспільства напрямі. Водночас, додаткове поширення кримінально-правових норм на ті відносини, які вже є в КК України, потенційно може створити ситуацію, за якої професія лікаря розглядатиметься з позиції високого ступеня ризику кримінальної відповідальності, з точки зору їх специфічних повноважень і методів виконання професійних обов'язків.

Література

1. Кримінальний кодекс України від 05.04.2001 р. № 2341-III // Відомості Верховної Ради України. - 2001. - № 25 - 265 с.

2. Ахметшин Р.Л. Уголовный кодекс для врача. - Донецк: Издатель А.Ю. Заславський, 2010. - 128 с.

3. Ахметшин Р.Л. УК в медицине. Взгляд врача на составы преступлений в медицинской сфере. - Донецк: Издатель А.Ю. Заславський, 2007. - 56 с.

4. Нагорна А.М., Степаненко А.В., Морозов А.М. Проблема якості в охороні здоров'я: Монографія. - Кам'янець-Подільський: Абетка-НОВА, 2002. - 384 с.

5. Кибальник А.Г., Старостина Я.В. Актуальные проблемы ответственности медицинских работников. - М.: ИЛЕКСА, 2006. - С. 92.

6. Стельцов Є.Л. Евтаназія: духовні, моральні та правові складові // Юридичний вісник України. - 2009. - № 16 (720). - С. 47.

7. Тимофеев И.В. Леонтьев О. Медицинская ошибка: медико-организационные и правовые аспекты. - СПб.: Издательство ДНК, 2002. - 80 с.

Кварталова В.В.
аспірант кафедра кримінального права, кримінального процесу та криміналістики Одеського національного університету ім. І.І. Мечникова
Надійшла до редакції 21.05.2011

УДК 004.056.53+378.14

ПРОБЛЕМИ ФОРМУВАННЯ ЗНАНЬ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЇХ РОЛЬ У ЖИТТІ СУСПІЛЬСТВА (НА БАЗІ ПОРІВНЯЛЬНОГО АНАЛІЗУ СИТУАЦІЇ У ПРОВІДНИХ КРАЇНАХ СВІТУ І В УКРАЇНІ)

Соколов А. В.

Стрімке зростання глобального інформаційного співтовариства, що відбувається в останній час, поставило під сумнів існування міждержавних кордонів з точки зору інформаційних потоків [1], які щомиті звертаються в обчислювальних системах, як у межах держав, так і випливають далеко за їх географічні кордони. Цей процес ознаменував перехід до нової моделі постіндустріального інформаційного суспільства. Важливою і невід'ємною складовою життя людини в інформаційному суспільстві є істотне подолання географічних відстаней, тобто мінімізація часу доступу до інформації. Це відбувається на тлі стрімкого зростання кількості користувачів віртуального простору [14]. Так за 2009 р., за даними дослідницького агентства InMind [3] кількість регулярних користувачів Інтернет в Україні збільшилася на 2,2 млн. осіб, склавши аудиторію з більше ніж 10,4 млн. осіб. А це, у свою чергу, призводить до лавиноподібного зростання кількості інформації, що зберігається в обчислювальних системах, або звертається в обчислювальних мережах. Звичайно, усе зазначене призводить до дедалі більшої актуалізації проблем безпеки інформації.

Рівень інформаційної безпеки як у державних структурах, так і у сфері господарської діяльності багато в чому визначається якістю підготовки працюючих в цій

галузі фахівців [9]. Тому однією з найгостріших сторін проблеми захисту інформації можна назвати саме підготовленість персоналу зайнятого у сфері створення, редагування та зберігання конфіденційної інформації. За оцінками фахівців, 85 % випадків порушення конфіденційності інформації вчинюються з вини людини [2], і, принаймні, 8 з 10 випадків можна було б запобігти за допомогою грамотного втручання фахівця. Причому важливу роль відіграє не тільки створення правильно організованої служби інформаційної безпеки, як на рівні підприємств, так і на рівні держави, що складається з професіоналів у цій галузі, а і рівень підготовки кожного з учасників процесу створення, редагування та зберігання конфіденційної інформації.

Аналіз робіт дослідників провідних країн світу (М. Кабай, М. Мотсіді, І. Гамбург, С. Азадеган) та вітчизняних фахівців (В.І. Слепцов, З.Н. Курлянд), які вивчають проблеми формування знань у галузі інформаційної безпеки, дозволяє здійснити оцінку ступеня розвитку української системи освіти порівняно з провідними країнами світу. Розгляд методологічних розробок фахівців університетів світу, які займаються даними проблеми, сучасних статистичних звітів, дає можливість розкрити сутність провідних сучасних методів оволодіння цією професією.

Виходячи з актуальності теми та проведеного аналізу досліджень у цій галузі, виділимо наступні цілі статті.

1. Виокремити недоліки в системі підготовки студентів у напрямку інформаційної безпеки.

2. Проаналізувати досвід вирішення наведених проблем у таких країнах як США, Великобританія, Німеччина, Австралія, Малайзія, та актуальність його застосування в Україні.

Розвиток ситуації за сценарієм переходу до глобального інформаційного суспільства робить завдання гарантування безпеки закритої інформації особливо важким і надзвичайно важким, якщо така інформація обертається в системах, поєднаних з глобальною й загальнодоступною мережею Інтернет.

Взагалі, з точки зору інформаційної безпеки інформацію можна класифікувати за наступними категоріями:

1. Загальнодоступна інформація. Така інформація може запускатися в обіг без будь-яких обмежень щодо її використання.

2. Інформація для внутрішнього користування. Зовнішньому доступу до цих даних має бути запобігнуто, але наслідки від того, що дані стануть загальнодоступними не є критичними.

3. Конфіденційна інформація. Дані, що належать до цього класу, є конфіденційними всередині організації, держави або іншого власника інформації, і доступ до них неавторизованих користувачів може призвести до серйозних наслідків.

4. Секретна інформація. Несанкціонований зовнішній або внутрішній доступ до цих даних матиме вирішальне значення для власника інформації. Кількість людей, які мають доступ до цих даних, повинно бути мінімальною.

Зрозуміло, що інформація, що належить до всіх категорій, крім першої, є закритою в загальному розумінні і вимагає відповідних заходів, що перешкоджають її розголошенню. А ефективність зусиль, спрямованих на збереження стану захищеності інформації, залежить не тільки від рівня технічного забезпечення, а й, перш за все, від уміння виявляти загрози, оцінювати рівень безпеки інформації та, виходячи із цього, розробляти і впроваджувати системи захисту на основі вимог законодавства України та міжнародних стандартів [9]. Ця обставина висуває певні вимоги до осіб, зайнятих обробленням і зберіганням закритої інформації, а також до співробітників, які безпосередньо забезпечують її захист.

Щоб зрозуміти основні знання, життєво необхідні співробітникам, які оперують закритою інформацією, залежно від рівня їх доступу, можна розглянути основні знання та вміння, необхідні для здійснення захисту інформації.

Дослідники університету, м. Тоусон, США, переконані, [4] що пізнання та досвід фахівця в галузі інформаційної безпеки, перш за все ґрунтуються на фундаменті теоретичних знань, а також на навичках у галузі програмування та участі в прикладних проектах. Незважаючи на те, що останнє вимагає значних витрат часу від викладача, припускаючи індивідуальну роботу, участь молодих фахівців у таких проектах є імперативом. Тим більше, як акцентує український дослідник педагогіки З.М. Курлянд [11], спільна робота викладача зі студентом (а індивідуальний підхід передбачає саме такий діалог), провокує розвиток не тільки того, хто навчається, тим самим подвоюючи користь, яку потенційно галузь може витягти з процесу підготовки фахівців.

Важливо, щоб методи викладання були адекватні матеріалу, що викладається. Так, на думку дослідників Маллакайського технічного університету, Малайзія, традиційний лекційний підхід є найбільш практичним [6] у викладанні дисциплін, що мають істотне теоретичне навантаження, наприклад, у криптографії. Цей підхід дозволяє ефективно охоплювати велику кількість базових і фундаментальних положень, однак він вносить у процес навчання певну пасивність з боку студентів, а також суттєво ускладнює зворотний зв'язок. З іншого боку, упровадження ведення конспектів дозволяє додати елемент активності, коли студент бере відповідальність за короткі записи під час лекції і на базі цього зможе зробити після або під час лекції короткий виклад засвоєного матеріалу. Останнім часом дедалі більш поширеним стає експертний метод, що припускає, що університет запрошує досвідченого фахівця, який працює в індустрії, як лектора чи інструктора проведення лабораторного практикуму. Такі фахівці, які є експертами у своїй галузі, дають вузько спеціалізовані заняття. Даний підхід, що широко розповсюджений в Австралії і Великобританії [7], показав хороші результати, оскільки також дозволяє максимізувати співробітництво університетів та промисловості. На жаль в Україні такий зв'язок між вищими навчальними закладами та промисловістю був істотно втрачений, що дуже погано позначилося як на якості підготовки фахівців, так і на самій промисловості. Це посилилося тим, що період бурхливого розвитку інформаційних технологій збігся в часі з розпадом Радянського Союзу [8]. Така обставина зумовила те, що формування вітчизняної системи підготовки кадрів у галузі захисту інформації значно відстає від темпів розвитку інформаційних технологій, більшість з яких була імпортовано в нашу країну.

Наступний метод - консультативний, що часто використовується, коли необхідну інформацію легко отримати, наприклад, з електронних джерел. Такий підхід дає найбільшу свободу учням. Часто при застосуванні даної методології студенти отримують на початку семестру завдання на виконання певного проекту або теми, які повинні бути досліджені. При підготовці фахівців у сфері інформаційної безпеки доцільно використовувати синтетичну методологію, що об'єднує, принаймні,

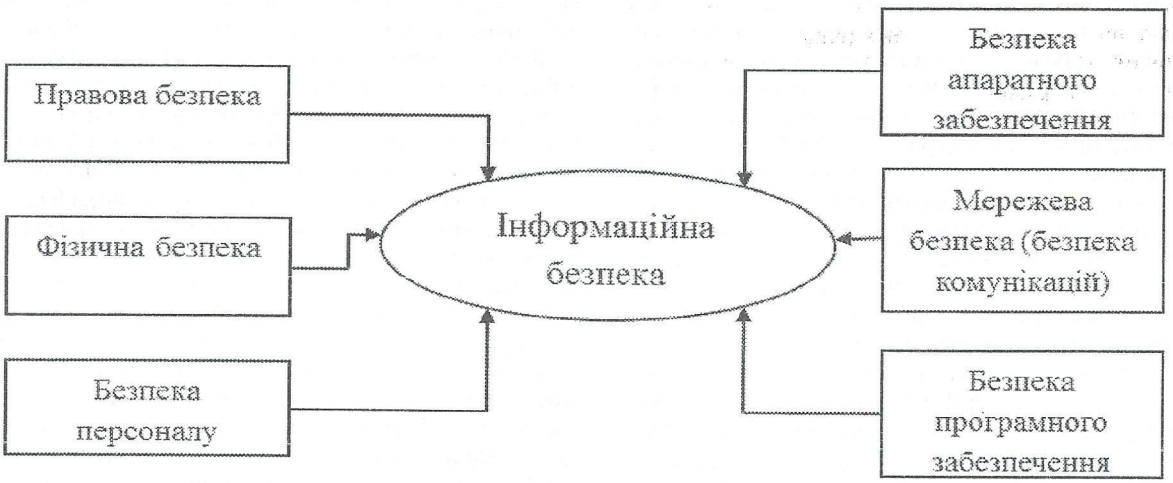

Рис. 1. Основні складові інформаційної безпеки

всі наведені, оскільки знання у сфері інформаційної безпеки представляють собою досить складну систему [5], яка ґрунтується на таких дисциплінах, як архітектура обчислювальної техніки, право (кримінологія, криптографія, програмування) веб-програмування, операційні системи, бази даних, взаємодія людини з комп'ютером, теорія передачі інформації, військові науки, бізнес та управління, філософія, етика, теорія ймовірностей і багато інших. Так в університетах США [12], крім наведених теоретичних дисциплін, акцентують увагу на оволодінні базовими практичними навичками зі спеціальності, такими як вивчення вузлів безпеки різних операційних систем, принципів роботи криптографічних алгоритмів і т.д. Дуже велика увага приділятиметься проведенню практичних занять, семінарів, різних змагань. У країнах Західної Європи також проводяться щорічні "змагання хакерів", що дозволяють пожвавити теорію й забезпечити студентів необхідним практичним багажем, як наприклад, у Дармштадському технологічному університеті, Німеччина [13].

Узагальнюючи, можна виділити основні складові здійснення захисту інформації, показані на рис. 1.

Зазначимо, що канали витоку інформації, які припускають крадіжку без застосування фізичного доступу, викликали найбільше число актів витоку інформації у 2010 р. [8]. Тому, буде доцільно розглянути, формування знань у галузі інформаційної безпеки з точки зору комп'ютерної безпеки. На думку дослідників США, підготовка фахівця в цій галузі повинна починатися з вивчення теоретичних основ, вивчення основних дисциплін, і переходити в розбір конкретних ситуацій, з якими фахівець може згодом зіткнутися на практиці. Древо придбання знань фахівцями в області інформаційної безпеки, спроектоване на традиційні галузі комп'ютерних наук, можна представити у вигляді схеми, показаної на рис. 2.

Розглянемо основні складові теоретичної основи інформаційної безпеки [15].

1. Курс мережевої безпеки розглядає основні прото-

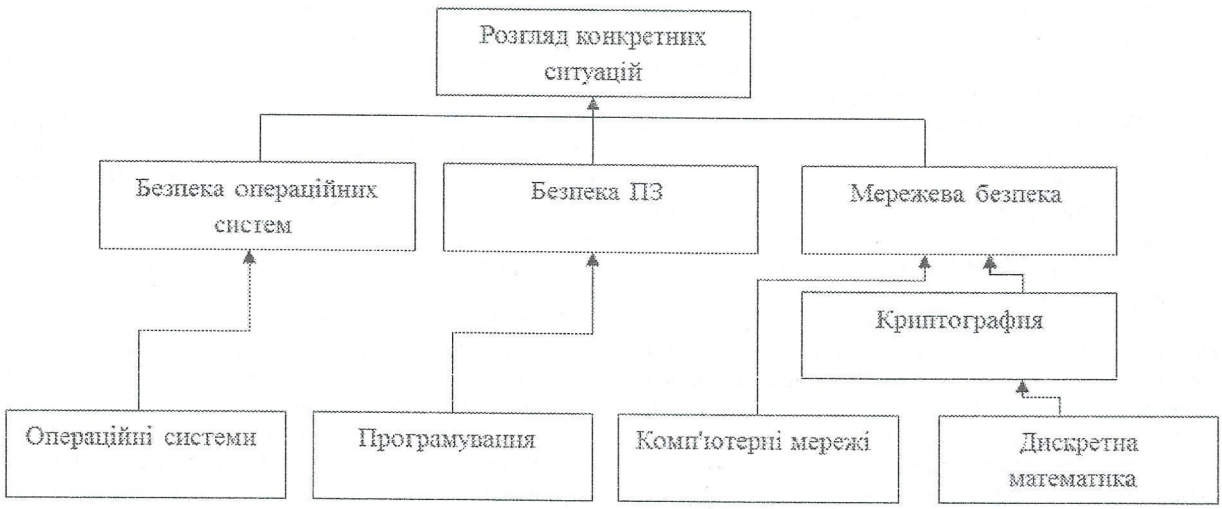

Рис. 2. Древо набуття знань у галузі інформаційної безпеки з точки зору комп'ютерної безпеки

Таблиця 1

Стислий план інтенсивного тренінгу

День	Лекція 1	Лекція 2	Лабораторний практикум
Тиждень 1	Вступ	Безпека апаратного забезпечення	Апаратне забезпечення ПК
1			
2	Веб програми	Веб програми	Веб програми
3	Переповнення буфера	Інші помилки при програмуванні	Переповнення через діяльність шкідливого коду
4	Сучасні шкідливі коди	Побудова мереж	Мережеве програмування
5	Прослуховування мережі (сніфінг)	Отримання доступу обманним шляхом, DoS, DDoS	Отримання доступу обманним шляхом, "спуфінг"
Тиждень 2	Мережеві топології	Застосування контрольних сум	Фізичні основи побудови мереж
1			
2	Bluetooth	Атаки по бездротових мережах	Дослідження безпеки бездротових мереж
3	Приховані дані	Мережі-приманки	Дослідження безпеки бездротових мереж
4	Аудит ІБ	Робота над проектами	Робота над проектами
5	Робота над проектами	Робота над проектами	Робота над проектами
Тиждень 3	Різнобічні експертизи ІБ	Експертизи НЖМД	Експертизи, аудит ІБ
1			
2	Експертизи НЖМД	Експертизи НЖМД	Експертизи, аудит ІБ
3	Шкідливе ПЗ	Шкідливі коди в Unix системах	Мережі-приманки
4	Екскурсія	Екскурсія	Екскурсія
5	Моделювання атак	Моделювання атак	Моделювання атак

коли автентифікації (наприклад, такі як Kerberos), основи безпеки електронної пошти, набір протоколів захисту даних, переданих по міжмережевому протоколу IP (IPsec), криптографічні протоколи, що забезпечують безпечну передачу на транспортному рівні (TLS / SSL), принципи роботи міжмережевих екранів і їх конфігурування.

2. Курс безпеки програмного забезпечення націлений на освоєння майбутніми фахівцями основних концепцій створення безпечного коду. Найбільш значними його частинами є аспекти безпеки при застосуванні мов програмування високого рівня, мов сценаріїв, а також безпека баз даних і веб-програм.

3. Дисципліна "Безпека операційних систем" покликана надати базові знання про те, як убезпечити обчислювальну систему на рівні операційної системи. Важливо, щоб у процесі вивчення курсу розглядалися найбільш поширені у світі операційні системи (Windows, *nix, Mac OS і т.д.) [4].

На жаль, потрібно відзначити, що в нашій країні, в більшості навчальних закладів [9] не склалося єдиного уявлення про необхідність викладання такої дисципліни як правові основи захисту інформації, не дивлячись на вельми успішне викладання дисциплін, пов'язаних з методами закриття фізичних і програмних каналів витоку інформації, криптографічних методів захисту інформації та подібних. А легітимність застосування тих чи інших організаційних чи технічних методів захисту інформації є однією з найважливіших домінант, що визначають їх вибір і застосування. Тому без введення хоча б основних тез курсу правого захисту інформації діяльність навіть висококласних фахівців у цій галузі часто може мати неправовий характер з усіма наслідками, що звідси випливають.

Інша серйозна проблема полягає у відсутності виходу на обґрунтування і формування проблем інформаційної безпеки з гуманітарної точки зору. Це, у першу чергу, стосується питань перепідготовки кадрів, зайнятих у галузі боротьби з комп'ютерними злочинами, і вимагає залучення до процесу дослідження проблем інформаційної безпеки методологічних апаратів гуманітарних наук.

Просту, але обґрунтовану програму підготовки розробили дослідники Ахенського університету, Німеччина [10]. Курс складається з 3-х тижнів інтенсивних занять. Дослідники припускають участь у курсі студентів з різними рівнями підготовки, різних спеціалізацій, що сприяє більш ефективному обміну знаннями. Проведення таких тренінгів може бути актуальним і для нашої країни, тому наведемо спрощений і систематизований план занять у таких групах у табл. 1 [10].

Спочатку застосування такої програми передбачало роботу студентів з 8:45 до 18:30. Після закінчення занять кожний студент повідомляв про набуті ним за день навички і знання. Проте зацікавленість учнів перевершила при роботі за таким планом усі очікування, багато студентів, захоплені роботою над своїми проектами, залишалися в лабораторіях після занять. Ймовірно, та-

Таблиця 2

Статистика по каналах витоку інформації

Канал витоку інформації	Частка інцидентів, %	
	Навмисних	Ненавмисних
Портативні комп'ютери	5.9	13.6
Портативні накопичувачі інформації	9.7	7.1
Персональні комп'ютери (безпосередній доступ)	12.4	36.1
Інтернет (включаючи електронну пошту)	31.4	13.6
Відбитки документів	33.5	8.3
Заархівована інформація	1.1	1.2
Інші канали	3.8	9.5
Нез'ясований канал	2.2	10.7

кий тренінг по ефективності використання часу та інформаційного навантаження набагато перевершує стандартні форми навчання, застосовувані в університетах.

Звичайно, у будь-якому випадку організація всіх складових захисту інформації, включаючи правову, є прерогативою співробітників-фахівців у цій галузі. Однак безпека інформації - відповідальність кожного, хто, так чи інакше, має до неї певний рівень доступу. Тому важливо, щоб такі службовці мали, як мінімум, початковий рівень знань у цій галузі.

Дослідник М. Маккайліп виділяє наступні базові знання й уміння, необхідні кожному співробітнику, який має доступ до конфіденційної інформації:

- базові знання міжмережевих екранів, антивірусного ПЗ і ПЗ для захисту від інших типів шкідливого коду, базові знання щодо методів знищення інформації;
- безпека портативних пристроїв зберігання інформації (диски, флеш-накопичувачі, КПК та інші);
- безпека електронної пошти;
- безпека відбитків конфіденційної інформації;
- стимуляція відмови від використання сторонніх Інтернет ресурсів у робочий час;
- ведення і регулярний перегляд журналу (наприклад, за допомогою вбудованих в ОС або систему безпеки утиліт);
- чітке дотримання спеціальних інструкцій, запропонованих службою захисту інформації.

Такий набір знань продиктований, у першу чергу, хоча б статистикою каналів витоку інформації у світі за 2010 р., проілюстрованою в табл. 2 [9].

Однак, на жаль, питання складання відповідної програми підготовки, за допомогою якої будь-який службовець, навіть який не має спеціальної технічної освіти, міг би познайомитися з основами захисту інформації усе ще залишається відкритим для вітчизняних дослідників і викладачів.

Одним з вирішальних факторів, що визначають як результат заходів щодо захисту інформації, так і розвиток галузі інформаційної безпеки в цілому, є рівень підготовки фахівців у цій галузі та персоналу зайнятого обробленням і зберіганням закритої інформації. Підсумовуючи зазначене, можна дійти наступних висновків.

1. Усі проаналізовані роботи як вітчизняних дослідників, так і дослідників провідних країн світу сходяться на думці, що достатній рівень підготовки професіоналів у цій галузі може бути досягнутий лише шляхом вивчення теоретичної бази та оволодіння практичними навичками як у технічних, так і в правових і гуманітарних аспектах даної спеціальності.

2. У нашій країні утворився істотний розрив між системою вищої освіти і промисловістю, зумовлений розпадом Радянського Союзу. Це особливо негативно позначилося на формуванні галузі інформаційної безпеки на тлі того, що багато інформаційних технологій було імпортовано в Україну, і країна зіткнулася з проблемами захисту інформації пізніше розвинених держав світу. Однак такий розрив, можливо, вдасться частково подолати, врахувавши методики консультативного підходу, що активно застосовуються у Великобританії та Австралії.

3. Особливе значення має підготовленість не тільки фахівців у сфері інформаційної безпеки, а й рівень знань у цій галузі доступний іншим службовцям, які оперують закритою інформацією і тим самим є її носіями. Для України гостро стоїть проблема розроблення методичного плану додаткової освіти для таких співробітників. Маючи на увазі державні організації, найбільш масово ця проблема виявляє себе в необхідності перепідготовки кадрів, зайнятих у сфері боротьби з комп'ютерними злочинами [9]. Однак не менш гостро така проблема стоїть і в комерційних організаціях.

4. Фактично має значення базовий рівень знань у цій сфері кожного учасника процесу обміну інформацією (для постіндустріального суспільства, по суті, кожного громадянина). Це може означати наявність передумов для серйозного знайомства з усіма аспектами захисту інформації в рамках системи загальної освіти.

Проведене дослідження дає можливість отримати гносеологічну користь для вітчизняних фахівців, оскільки рішення ідентичних проблем, пов'язаних із захистом інформації з точки зору освіти в цій галузі, вироблені у провідних країнах світу, можуть бути також повністю або частково прийнятні й для України, що надало б нашій країні можливість дати гідну відповідь сучасним викликам постіндустріального суспільства.

Література

1. Малик І. Народження "Доктрини інформаційної безпеки України": від теорії до практики // Українська національна ідея: реалії та перспективи розвитку. - Львів: Вид-во Національного університету "Львівська політехніка", 2010. - 22-й вип. - С. 76-81.

2. Secretary of Defense, Acquisition, Technology and Logistics (2009). Military Critical technologies List. - Pentagon, VA, USA: Section 17, 2009. - P. 49. - MCTL-17-49.

3. Открытые результаты: "Аудитория регулярных пользователей Интернет в Украине" / Исследовательское агентство полного цикла InMind, представитель международной сети Factum Group в Украине. - [Электронный ресурс]: http://www.inmind.com.ua/upload/page_files/01.pdf.

4. Undergraduate computer security education / S. Azadegan, M. O'Leary, A. Wijesinha, M. Zimand // Towson University, 2005. - P. 11. - [Electronic resource]: http:/

/cisr.nps.edu/downloads/wecs7_ch2.pdf.

5. Approaches to the teaching of information security / I. Hamburg, O. Cernian, D. Mancas, A. Basandica // Duisburg University, 2005. - P. 5. - [Electronic resource]: http://www.iaq.uni- due.de/aktuell/veroeff/2005/hamburg03.pdf

6. Motsidi M.R. New Approach in Teaching Network Security Subjects / Mohammad Radzi Motsidi, Mohd Fairuz Iskandar Othman, Yahaya Abd Rahim, Mohd Najwan Khambari // International Conference on Information: Kuala Lumpur, Malaysia. - 2009. - 12-13 August. - [Electronic resource]: http://ici9.oum.edu.my/pdf/paper09.pdf.

7. Practice and Application Oriented Education in KUTKM / I. Hassan, M. Ayob, M. Sulaiman // Universiti Teknikal. - Malaysia, Melaka, 2005.

8. Infowatch(2010). Global Data Leakage Report. - Moscow, 2010. - P. 11. - [Electronic resource]: http://www.bisc.lv/files/pdf/Glob_utech_perv_pol%202010_eng.pdf.

9. Правовая подготовка кадров в области информационной безопасности / В.И. Слепцов, Л.М. Карпуков // Радіоелектроніка. Інформатика. Управління. - Запоріжжя, 2008. -№ 1. - С. 133-137.

10. Teaching Data Security at University Degree Level / M. Dornseif, F. Gaertner, M. Mink, L. Pimenidis. - [Electronic resource]: http://pi1.informatik.uni-mannheim.de/filepool/publications/teaching-data-security-at-university-degree-level.pdf.

11. Курлянд З.Н. Концепція мультиплікативності функціонування вищої школи як шлях до трансформації сучасного виміру системи вищої освіти України // Науковий вісник ПНПУ ім. К.Д. Ушинського. - 2010. - № 11-12. - С. 194-200.

12. Kabay M.E. Information Security Education Resources for Professional Development. - 2009. - P. 34. - [Electronic resource]: http://www.mekabay.com/overviews/infosec_ed.pdf.

13. Angewandte Informationssicherheit: Ein Hacker-Praktikum an Universitaten / M. Schumacher, M.L. Moschgath, U. Roedig. - B.: Informatik Spektrum, 2000. - P. 211.

14. Current state analysis and development prognosis for Internet technologies in Ukraine. Research program for prevention and counteraction to transnational computer incidents / V.A. Golubev, N.D. Krasnostup, V.K. Bronnikov. - Zaporozhye: Design Group, 2000. - P. 25.

15. A dedicated undergraduate track in computer security education / S. Azadegan, M. Lavine, M. O'Leary, A. Wijesinha, M. Zimand. - Massachusetts, USA: Kluwer Academic Publishers, 2003. - P. 319-331.

Соколов А.В.
студент Інституту радіоелектроніки та телекомунікацій Одеського національного політехнічного університету
Надійшла до редакції 01.04.2011

УДК 340.111.5

ДЕЯКІ НАПРЯМИ ОПТИМІЗАЦІЇ ПРОЦЕСУ ФОРМУВАННЯ ПРАВОСВІДОМОСТІ МОЛОДІ В УКРАЇНІ

Ткачук А. С.

Духовний розвиток людини має важливе значення для побудови самостійної незалежної Української держави з власними соціальними відносинами й правовою системою. Процес переходу до ринкових відносин, який розпочався в Україні після проголошення незалежності й триває досі, є не послідовним і суперечливим. Визнання приватної власності й розвиток нових приватних форм господарювання зумовлюють певні деформації в економічній сфері українського суспільства, які породжують деформовану свідомість, бездуховність і свавілля в різних сферах його життя. Такі тенденції особливо небезпечні для державної розбудови, створення її економічної, політичної й духовної бази.

Складна соціально-політична й економічна ситуація породила могутні соціальні, соціально-психологічні, економічні, соціально-побутові чинники дестабілізації правової свідомості всіх верств населення України, також і молоді. На жаль, за статистикою, серед молодого покоління українців спостерігається посилення правової неграмотності й правового нігілізму. Проблема полягає у відсутності цілісної ефективної системи правового виховання населення, що є однією з причин низького рівня правової свідомості суспільства. Про це свідчить кількісне зростання злочинності взагалі, та протиправної поведінки молоді, зокрема.

Мета наукового дослідження - визначити деякі напрями оптимізації процесу правовиховної діяльності з урахуванням сучасних реалій і проблем суспільного життя в Україні; обґрунтувати необхідність прийняття "Державної програми формування правосвідомості та правової культури молоді"; знайти можливі шляхи підвищення правосвідомості молоді за рахунок дослідження європейського досвіду у вирішенні подібних питань; виявити тенденції подальшого розвитку правосвідомості молоді.

Об'єктом наукового дослідження виступає правосвідомість молоді як особливої соціальної групи.

Предмет наукового дослідження - напрями оптимізації процесу формування правосвідомості молоді в Україні.

Наукова новизна дослідження полягає в обґрунтуванні необхідності створення в Україні протягом найближчого періоду загальної концепції формування правової свідомості і правової культури суспільства й прийняття "Державної програми формування правосвідомості та правової культури молоді". Також у статті досліджено особливості взаємозв'язку між економічним рівнем країни й правовою свідомістю її громадян, виявлено тенденції подальшого розвитку правосвідомості молоді.

Цю проблему досліджували такі вчені: О.Г. Данильян, Я.О. Овдієнко, В.І. Андрейцев, С.Є. Демський, В.П. Колісник, Л.О. Марченко, С.В. Матвєєв, О.О. Орлова, Л.М. Павловська, О.В. Петришин, С.П. Погребняк, С.Г. Серьогіна, Ю.М. Сміщук, В.Я. Тацій, Ю.М. Тодика та ін. Відповідні дослідження в рамках інших суспільних наук проводилися такими вченими, як Й. Васькович, В.Д. Воднік, О.П. Дзьобань, Л.М. Герасіна, В.І. Головченко, Є.І. Коваленко, О.П. Кондратюк, А. Кутиркін, Н.П. Осипова, М.П. Требін, М.П. Щербань та ін. Незважаючи на різні погляди щодо різних аспектів правового виховання, чітких уявлень щодо шляхів його вдосконалення в трансформаційний період розвитку суспільства на сьогодні в літературі майже не існує. Саме тому одним із завдань наукового дослідження є визначення