8. Рудницька О.П. Інтегративні зв'язки у викладанні предметів художньо-естетичного циклу //Початкова школа. — 2001. - №5. - С. 40-45.
9. Ушинский К.Д. Собр. соч. - М.: Изд-во АПН РСФСР, 1979. - Т. 5. - 592 с.
10. Щолокова О.П. Основи професійної художньо-естетичної підготовки. Монографія. — К.: 1996. — 172 с.

ЗНАЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНОМУ СУСПІЛЬСТВІ (НА ПРИКЛАДІ ПОРІВНЯННЯ ГАЛУЗІ В ПРОВІДНИХ КРАЇНАХ І УКРАЇНІ)

УДК 004.056.53.001.31

Соколов А.В.

У статті розкриваються проблеми становлення галузі інформаційної безпеки в Україні, проводиться порівняльний аналіз досягнутих результатів, а також сучасних тенденцій і проблем у розвитку даного напрямку. Розкриваються погляди дослідників провідних держав світу у галузі інформаційної безпеки.

В статье раскрываются проблемы становления отрасли информационной безопасности в Украине, проводится сравнительный анализ достигнутых результатов, а также современных тенденций и проблем в развитии данного направления. Раскрываются взгляды исследователей ведущих государств мира в области информационной безопасности.

This article is devoted to the problem of forming of a sector of information security in the Ukraine. The systemic analysis of achieved results and modern tendencies of the concerned problem is given. The scientific views of leading world researchers in the data security area are revealed.

Постановка проблеми в загальному вигляді ... У теперішній час в Україні йде активне впровадження інформаційних технологій [1] в усі сфери життєдіяльності нашого суспільства. Це обумовлює створення та поширення в обчислювальних мережах країни величезної кількості конфіденційної інформації, поданої в електронному вигляді. Наша країна зіткнулася з настільки масштабними проблемами захищеності даних пізніше, ніж провідні держави світу. Незважаючи на те, що рівень розвитку світової торгівлі, побудова економіки нашої держави на принципах ринкової саморегуляції, а також її членство в міжнародних торговельних організаціях, дозволяють підтримувати технічне оснащення галузі на досить розвиненому, принаймні, для сфери бізнесу рівні. Недостатній розвиток законодавчої бази, а також нестача висококваліфікованих кадрів представляють собою значну проблему.

Аналіз публікацій та досліджень ... Аналіз робіт як вітчизняних дослідників (Р. Калюжний, В. Голубєв), так і публікацій дослідників провідних країн світу (Т. Шмедінгхофф, А. Акквісті, М. Кебей, М. Шумахер), а також міжнародних і національних нормативних документів і стандартів дозволяють провести порівняльну оцінку розвитку галузі в Україні та передових державах світу.

Формулювання цілей статті ... Мета статті – огляд тенденцій розвитку нормативно-технічної документації, засобів і методів професійної підготовки фахівців, що застосовуються такими країнами як США, Канада, Великобританія, Німеччина, Австралія в області інформаційної безпеки. Проведена порівняльна характеристика методології, що застосовується в цих країнах. Це дозволяє отримати гносеологічну користь для вітчизняних фахівців, оскільки ідентичні проблеми, пов'язані із захистом інформації, що виникли у провідних країнах світу, знаходять свої повні та часткові рішення, які можуть бути також прийнятні і для України.

Виклад основного матеріалу дослідження ... В останні роки проблеми інформаційної безпеки в світі все більше набувають свою актуальність, стаючи проблемами кожного з нас. Це обумовлено в першу чергу тим, що в даний час робота цілих держав, бізнес структур, підприємств, так і діяльність окремих людей пов'язана із здійсненням угод або будь-яких операцій з грошима, а також приватною інформацією все частіше і частіше здійснюється в електронній формі, за допомогою використання мережевих технологій [3]. Створення, поширення та зберігання такої інформації істотно збільшує потенційну можливість несанкціонованого доступу, розкриття, підробки, а також випадкової втрати або руйнування цих важливих даних. Так, наприклад, дослідження проведені в Університеті Карнегі - Меллон (Пітсбург, штат Пенсільванія, США) вказують, що більш 67% споживачів «дуже стурбовані» рівнем секретності своєї персональної інформації, яка поширюється в комп'ютерних мережах [4].

У зв'язку з тим, що комп'ютерний ринок нашої держави отримав свій розвиток із значним запізненням порівняно із ринком інформаційних технологій країн Північної Америки та Західної Європи, відповідно українське суспільство зіткнулося з проблемами, пов'язаними з інформаційною безпекою пізніше розвинених країн. Так, унаслідок багаторічного та скрупульозного накопичення досвіду міжнародним співтовариством, у 2005 році ISO (Міжнародною організацією зі стандартизації) були сформульовані нові стандарти серії ISO / IEC 27000, також відомої як «ISMS Family of Standards» або «ISO27k». Дана серія, включає в себе 11 вже опублікованих нормативних документів, які за оцінками експертів, є кращим у світі практичним посібником з менеджменту інформаційної безпеки. Наприклад, стандарти ISO / IEC 27001, ISO / IEC 27002 повністю охоплюють захист інформації в таких галузях людської діяльності як телекомунікації, фінансові послуги, охорона здоров'я і подібних. Стандарти даної серії були позитивно оцінені світовою спільнотою, тому далі сталася поява еквівалентних національних стандартів в Австралії, Великобританії, Нової Зеландії, Бразилії, Чилі, Чеській Республіці, Данії, Естонії, Японії, Литві, Нідерландах, Росії та інших державах.

В нашій країні досі не існує уніфікованого стандарту, що регулює інформаційну безпеку в українському суспільстві [2]. В Україні було створено безліч (більше 260) нормативних документів, що регулюють сферу інформаційної безпеки. Вони є обов'язковими до виконання, якщо система інформаційної безпеки створюється для державних органів, таких як: система безпеки Кабінету Міністрів України, автоматизована система Державної податкової адміністрації та Рахункової палати Верховної Ради України, Єдиної бази статистичних даних та статистичної звітності Міністерства Статистики України, Єдиної Державної автоматизованої паспортної системи, Міжвідомчої інтегрованої інформаційно-анал-

ітичної системи правоохоронних органів, єдиної супутникової системи передачі інформації [1].

Однак, на жаль, така нормативна база не завжди є прийнятною для бізнес-структур. Основними недоліками вищезгаданих нормативних документів є:

1. Вимоги до систем захисту інформації часто є необґрунтовано завищеними, що знижує рентабельність вітчизняних підприємств.
2. Вимоги українських нормативних документів неповні і містять протиріччя [2].
3. Частина нормативних документів на сьогоднішній день застаріли, у зв'язку з чим втратили свою актуальність.
4. Вимоги наших національних нормативних документів орієнтовані на державні структури.

Потрібно відзначити, що на вітчизняному ринку представлено досить велику кількість необхідного обладнання для забезпечення належного захисту інформації. Тут можна виділити як системи фізичного захисту носіїв інформації, так і системи криптографічного захисту інформації, міжмережеві екрани. Варто зауважити, що понад 23% власників приватних будинків в Австралії, а також переважна більшість [5] комерційних організацій віддали перевагу використання охоронних сигналізацій для фізичного захисту своєї власності. В Україні цей показник залишається досить низьким, незважаючи на те, що сучасні системи таких охоронних сигналізацій, вироблені лідируючими на ринку компаніями, наприклад такими як Канадська «DSC» відрізняються низьким енергоспоживанням (енергоспоживання базових елементів систем і клавіатури не перевищує 4 Вт, енергоспоживання сенсора - 0.13 Вт), великою кількістю сенсорів, що підключаються, можливістю використання бездротових сенсорів, витонченими підсистемами самодіагностики охоронної системи. Фактично, сучасні охоронні сигналізації можуть гарантувати безпеку фізичного об'єкта.

Що стосується ринку програмного забезпечення, то варто зазначити, що більшість комерційного програмного забезпечення, що використовується практично у всіх сферах діяльності підприємств: електронна пошта (відомо, що 80% інтелектуальної власності компаній міститься саме в електронних повідомленнях, що створюються, одержуються і зберігаються компанією), системи бухгалтерського обліку, системи резервного копіювання, системи обміну файлами, системи передачі IM повідомлень, оглядачі Інтернет забезпечені криптографічним захистом персональної інформації, яка може бути передана через них. Наприклад, найбільш популярний у світі програмний продукт, який використовується для обміну електронними повідомленнями Microsoft Outlook Express (Windows Mail) забезпечено асиметричною системою шифрування S/MIME. Криптографічні системи програмних продуктів більшості виробників, що лідирують на світовому ринку, є дуже надійними. Тому, найчастіше, для українських підприємств вартість злому такої системи набагато перевищує вартість самої інформації, яку намагаються розкрити. Насторожує швидше той факт, що за оцінками міжнародної аналітичної компанії IDC рівень використання неліцензійних програмних продуктів приватними особами в нашій державі досяг 85% в 2009 році [6]. Цей показник виріс на 1%, в порівнянні з 2008 роком, завдавши нашій економіці збиток в 272 млн. доларів США за 2009 рік. У Західній Європі цей показник також досить високий, однак не перевищує 35%, і відповідно 22%

для Північної Америки (США і Канада). Зауважимо, що в Україні така ситуація склалася незважаючи на порівняно належним чином сформовану законодавчу базу щодо використання неліцензійного програмного забезпечення. Так, використання подібних продуктів в нашій країні, може потягти за собою адміністративну [7, стаття 51-2], а також кримінальну [8, стаття 176] відповідальність.

Недотримання прав інтелектуальної власності в нашій державі, не тільки створює серйозні перешкоди для технологічного та економічного розвитку країни і негативно впливає на її інвестиційну привабливість, але також створює серйозні загрози для безпеки інформації, що обробляється даними програмними продуктами. Оскільки будь-яке порушення цілісності коду третіми особами як не дає гарантії правильної роботи криптографічних алгоритмів системи, так і значно підвищує ймовірність включення в програмний продукт закладок, що дозволяють зловмисникові отримати доступ до конфіденційної інформації, повністю компрометуючи розгорнені системи захисту.

Проте, за оцінками американських фахівців, більше 85% випадків порушення секретності інформації відбувається з вини людини. Так, у сегменті бізнесу, 8 з 10 випадків можна було б запобігти за допомогою грамотного втручання фахівця [9]. Тому не можна недооцінювати вплив якості освіти на галузь інформаційної безпеки в Україні. В університетах США, при підготовці студентів, які обрали своєю спеціальністю «Інформаційну безпеку» робиться наголос на оволодінні студентами базових дисциплін, пов'язаних з їх спеціальністю, таких як інформатика, логіка, структура даних, програмування, криптографія [10]. І вже з першого семестру проводяться навчання спеціальним навичкам: вивченню вузлів безпеки різних операційних систем, принципів роботи криптографічних алгоритмів. Велика увага приділяється проведенню практичних занять, семінарів, різних змагань. Так, наприклад, в Дармштадському Технологічному Університеті (Німеччина) щорічно проводяться «Змагання Хакерів», які мають місце в лабораторіях Університету. Студенти діляться на команди, кожна з яких повинна правильним чином налаштувати безпеку своїх комп'ютерних систем, і, використовуючи методи, отримані в результаті прослуховування курсів лекцій провести атаку на комп'ютерну систему команди-супротивника [11]. Після таких атак кожна з команд аналізує атаки на свої системи і намагається поліпшити свою систему безпеки. Схожі лабораторні практикуми проходять [12] і у Військовій Академії у Вест-Пойнті, США.

Висновки ... Досвід, накопичений країнами, які раніше почали формувати рішення проблем захисту інформації, може бути застосований і в Україні. У нашій країні можлива підготовка і прийняття уніфікованої нормативної бази, яка дозволить чітко регулювати розгортання систем інформаційної безпеки для бізнес-структур, гнучко відповідаючи їх вимогам. Застосування досвіду передових країн в підготовці та професіоналізації фахівців у галузі інформаційної безпеки, надасть нашій країні можливість дати гідну відповідь сучасним проблемам інформаційного суспільства.

Література

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

2. Калюжний, Р.А. Щодо питань реформування законодавства у сфері суспільних інформаційних відносин [Текст] / Р.А. Калюжний, В.Д. Гавловський, М. В. Гуцалюк, В.С. Цимбалюк . – К.: КМ «Academia», 2001. – с. 164.

3. Smedinghoff, T.J. The state of information security law [Text] / T. J. Smedinghoff. – Bristol, PA, USA : Taylor & Francis, Inc, 2008. – p. 52 Bibliography: p.48-52. – ISSN: 0736-6981.

4. Acquisti, A. Privacy in electronic commerce and the economics of immediate gratification [Text] / A. Acquisti, R. Gross. – New York, NY, USA : ACM Press, 2005. – p. 108 – ISBN: 1-59593-228-3.

5. Australian Bureau of Statistics (2000). Home Security Precautions New South Wales [Text]. – New South Wales : report number 4516.11, 2000 – p. 16. – ISBN: 0 642 54275 9.

6. Международная аналитическая компания IDC Украина // http://www.idcukraine.com/

7. Україна. Закони (2001). Кримінальний кодекс [Текст]: – К. : Правова Єдність, 2010. – с. 152.

8. Україна. Закони (2001). Кодекс про адміністративні правопорушення [Текст]. – Харків : Парус, 2009. – с. 252 – ISBN: 978-966-8482-52-6 .

9. Secretary of Defense, Acquisition, Technology and Logistics (2009). Military Critical technologies List [Text]: – Pentagon, VA, USA : Section 17, 2009. – p. 49. – MCTL - 17-49.

10. Kabay, M. E. Information Security Education Resources for Professional Development [Text]. / M. E. Kabay, PhD. – 2009. – p. 34. // http://www.mekabay.com/overviews/infosec_ed.pdf

11. Schumacher, M. Angewandte Informationssicherheit: Ein Hacker-Praktikum an Universitaten [Text] / M. Schumacher, M.L. Moschgath, U.Roedig. – B.: Informatik Spektrum, 2000. – p. 211.

12. Dodge, R. C. Organization and training of a cyber security team [Text] / R. C. Dodge, D. J. Ragsdale, C. Reynolds. – Germany, Frankfurt : IEEE Press, Man & Cybernetics, 2003. – p. 18. – ISBN: 0-7803-7952-7.

ПРОФЕСІЙНО ОРІЄНТОВАНЕ НАВЧАННЯ ЗАСОБАМИ ДІАЛОГІЧНИХ СИТУАЦІЙ НА ЗАНЯТТЯХ У ВИЩИЙ ШКОЛІ

Вишневська К. Г.

В статті розглянуто зміст професійно–орієнтованого навчання, який характеризується розвиненою здатністю до розв' язання професійних задач, розвиненим мисленням і свідомістю. Ми розглядаємо професійно-орієнтоване навчання як здатність студента економічного ВНЗ до самовдосконалення; оволодіння знаннями з міжнародної економіки та як складне особистісне утворення, що включає в себе структурні компоненти, якості особистості, які впливають на мотиваційну сферу. Зміст професійно-орієнтованого навчання становлять соціально значущі мотиви професійної діяльності; педагогічні здібності; повнота, глибина економічних та психологічних знань і вмінь; соціальна активність особистості майбутнього фахівця економіки.

***Ключові слова**: професійно орієнтоване навчання, діалогічні ситуації.*