

УДК 004.85: 004.031.

Михайло КОЛЯДА

## ПРОФЕСІЙНА ПІДГОТОВКА ФАХІВЦІВ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ У США

*У статті розглядається професійна підготовка фахівців із захисту інформації та управління інформаційною безпекою у Сполучених Штатах Америки. Показано сутність та особливості педагогічних систем підготовки фахівців такого профілю в американських вищих навчальних закладах.*

*В статье рассматривается профессиональная подготовка специалистов по защите информации и управления информационной безопасностью в Соединенных Штатах Америки. Показана сущность и особенности педагогических систем подготовки специалистов такого профиля в американских высших учебных заведениях.*

*We consider the training of specialists in information security and information security management in the United States. Displaying the nature and features of educational systems of the kind of training in American universities.*

Вивченню методології підготовки спеціалістів із захисту інформації та управління інформаційною безпекою за рубежом науковці України почали приділяти свою увагу в 1994 р., коли для забезпечення мобільності фахівців на ринку праці поєднали споріднені спеціальності та відкрили нові спеціалізації. Тоді Міністерство освіти України спільно з комітетом Держкомсекретів України здійснило упорядкування Переліку напрямів підготовки фахівців, який постановою Кабінету Міністрів України від 18 травня 1994 р. № 325 було затверджено. Вводилися такі спеціальності: «Технічні системи захисту інформації» (напрямок – Радіотехніка), «Комплексні системи захисту інформації» (напрямок – Прикладна математика), «Адміністративний менеджмент у сфері захисту інформації з обмеженим доступом» (напрямок – Менеджмент), «Захист інформації з обмеженим доступом» (напрямок – Соціологія), «Захист інформації з обмеженим доступом та автоматизація її обробки» (напрямок – Комп'ютеризовані системи, автоматика і управління).

Перші наукові статті були присвячені обґрунтуванню і доцільності реформування системи підготовки фахівців такого профілю (Г. Лазарев, С. Кльоцкін, В. Хорошко, О. Богданов, О. Додонов, О. Корнейко, В. Мохор, Г. Маклаков, Е. Рижков, В. Ворожко й ін.). На початку ХХ ст. стан підготовки фахівців у сфері інформаційної безпеки розглядали вчені К. Беляков і В. Павловський. Однак вивченню системи такої підготовки за кордоном, зокрема в США ніхто з науковців не приділяв достатньої уваги.

Ця тема залишається мало вивченою і сьогодні, хоча розробка її дуже актуальна і своєчасна. Зараз готуються державні стандарти вищої освіти України у вигляді вимог до підготовки фахівців освітньо-кваліфікаційного рівня бакалавр і магістр напрямку підготовки 1701 «Інформаційна безпека».

**Метою статті** є розкриття сутності педагогічної системи підготовки фахівців із захисту інформації та управління інформаційною безпекою у США.

Для того, щоб простежити ці суттєві відмінності, треба виокремити той інваріант в структурі педагогічної підготовки США, який би дозволив оцінити її ефективність. Головним елементом такого інваріанта є зміст освіти, що проявляється через вимоги до системи знань, умінь та навичок, які необхідні фахівцеві такого профілю.

Зараз в Україні спеціалістів із захисту інформації та управління інформаційною безпекою готують за одним напрямом 1701 «Інформаційна безпека», що містить три спеціальності – «Безпека інформаційних і комунікаційних систем» (6.170101, 8.170101), «Системи технічного захисту інформації» (6.170102, 8.170102), «Управління інформаційною безпекою» (6.170103, 8.170103) [1]. Повного аналога такого напрямку підготовки фахівців в американських ВНЗ США

не існує. Найбільш близькими за змістом та ідеями, що лежать в основі підготовки фахівців в галузі інформаційної безпеки у США, є комп'ютерні й інженерні науки, оскільки вони є базовим ядром дисциплін професійної підготовки таких фахівців.

У 90-і роки XX ст. створений міжнародний галузевий освітній стандарт (curriculum standards) серії комп'ютерних навчальних планів – Computing Curricula (CC91: <http://www.acm.org/education/curr91/homepage.html>), в якому були дані рекомендації щодо складання навчальних планів та програм чотирирічної підготовки бакалаврів у комп'ютерних науках (Computer Science) і комп'ютерної інженерії (Computer Engineering). Він став основою для розробки нової програмної серії підготовки фахівців, що пов'язані з використанням інформації різних видів за допомогою комп'ютерної та комунікаційної техніки.

Ще у 1964 р. було створено організацію Computer Society («Суспільство епохи комп'ютеризації»). Це технічне співтовариство, що разом з комітетом американського Інституту інженерів-електриків (IEEE) фокусує свою увагу на інженерно-технічній складовій використання комп'ютерної техніки, з огляду при цьому на інженерні перспективи. На сьогоднішній день членами Computer Society є інженери-розроблювачі апаратного забезпечення (Computer Engineers), інженери-розроблювачі програмного забезпечення (Software Engineers), комп'ютерні технологи (Computer Technologists) і вчені з комп'ютерних наук (Computer Scientists). З 1977 р. ця організація займається розробкою рекомендацій щодо складання навчальних планів.

На рубежі XX-XXI ст. в англomовних країнах з'явилася нова дефініція – «комп'ютинг» (*computing*), що стала широко використовуватися не тільки в цих країнах, а й далеко за їх межами. Завдяки засобам масової інформації, сучасним комунікаціям і мережі Інтернет, цей термін проникнув і почав самозатверджуватися спочатку в російськомовному, а тепер і в україномовному науковому й освітньому середовищі. За своїм значенням він дуже точно відображає широкий пласт наукової і практичної діяльності, пов'язаної з використанням і застосуванням засобів комп'ютерної і комунікаційної техніки, обчислювально-математичних методів та інформаційно-програмних засобів обробки, збереження, передання і захисту інформації, упровадження нової науково-технічної інженерної думки на грані відкриттів у математиці, фізиці, хімії, біології, психології, лінгвістиці та інших науках. У документі «Computing Curricula 2005» [2, с. 9] цей термін визначається так: «Комп'ютигом називається будь-яка цілеспрямована діяльність, яка потребує комп'ютера й одержує з нього користь, а також створює сам комп'ютер». Ось неповний список того, що містить у собі поняття «комп'ютинг»: проектування і побудова апаратного забезпечення і систем програмного забезпечення; обробка, структурування і управління різними видами даних; виконання наукових досліджень з використанням комп'ютера; штучний інтелект у комп'ютерних системах; створення і використання технічних та програмних комунікаційних, інтерактивних і мультимедійних засобів; захист інформації від несанкціонованого доступу і багато іншого.

Ще в рамках першої версії цього документа, з'явилися наступні напрями з підготовки фахівців з комп'ютингу: 1) *Комп'ютерна наука* (Computer Science – CC2001) – підготовлено в 2001 р.; 2) *Інформаційні системи* (Information Systems – IS2002) – підготовлено в 2002 р.; 3) *Розробка програмного забезпечення* (Software Engineering – SE2004) – підготовлено в 2004 р.; 4) *Комп'ютерні розробки* (Computer Engineering – CE2004) – підготовлено в 2004 р. Потім до них додалися ще два напрями, які підготовлено в 2006 р.: 5) *Інформаційні технології* (Information Technology – IT); 6) *Інформаційний менеджмент* (Information Management – IM).

Для кожної з вищезгаданих шести програм створено рекомендації до складання навчальних планів підготовки випускників бакалаврського рівня. Ці рекомендації прийнято і схвалено міжнародним співтовариством викладачів і фахівців з комп'ютингу. На цих рекомендаціях базується структура освітнього процесу не тільки в США, а й в багатьох ВНЗ країн.

У рамках цих шести міжнародних напрямів з комп'ютингу почалася розвиватися підготовка в сфері захисту інформації та управління інформаційною безпекою (Рис. 1). Особливо ця активізація розпочалася після трагічних подій 11 вересня 2001 р. в Нью-Йорку. Відтоді в багатьох регіонах США почали регулярно проводитися семінари, конференції, симпозіуми з проблем кіберзлочинності і кібертероризму. Для удосконалення методів навчання Пентагон створив спеціальний підрозділ – «Управління програмами з інформаційної безпеки»

(Information Assurance Program Office). В рамках національної безпеки (NSA) ще в 1999 р. були сформовані центри післядипломної освіти і почало функціонувати «Агентство із захисту інформаційних систем» (Defense Information Systems Agency – DISA). В 2000 р. до цих центрів підключено 14 провідних університетів США [3]. Стало очевидним, що проблеми державного забезпечення інформаційної безпеки набувають транснаціонального характеру і вимагають консолідації та координації зусиль всіх країн у справі підготовки фахівців із захисту інформації та управління інформаційною безпекою. Тому одним із напрямків удосконалення системи підготовки фахівців у цій сфері в США бачать у створенні міжнародних об'єднань. Ця країна ініціювала створення мережі міжнародних консорціумів з питань підготовки кадрів в галузі захисту інформації. Найкрупнішим з них є Міжнародний консорціум із сертифікації в галузі безпеки інформаційних систем (International Information Systems Security Certification Consortium, Inc.), що базуються у Відні та Вірджинії [4], а також: Мережна академія CISCO (де CISO: Chief Information Security Officer – Головний офіцер інформаційної охорони або Директор з інформаційної безпеки).

Американські ВНЗ прагнуть відповідати найбільш передовим вимогам у сфері теоретичних розробок і практичних досліджень. Тут краще, ніж у Європі, технічне оснащення навчального процесу, а можливості для дослідника-початківця необмежені і вже самі собою стимулюють його інтерес до обраної спеціальності. У кожній лекційній аудиторії – комп'ютер, проектор, відеопроєктор, відеомагнітофон, аудіоапаратура. Багато європейських світил у різних областях знань вважають за честь прийжджати сюди і читати лекції, тоді як американські ВНЗ мають виняткові матеріальні можливості запрошувати їх на свої кафедри. У рейтингу вищої освіти зі 100 кращих університетів світу американські займають 70–80 позицій.

Офіційних рейтингів кращих американських ВНЗ у цій країні не існує. Однак існують рейтинги за окремими напрямками. Так, серед факультетів, що готують фахівців у галузі комп'ютерних технологій, визначена наступна десятка кращих ВНЗ (за матеріалами довідника F1 Study, 2005): 1. Стенфордський університет (Stanford University); 2. Массачусетський технологічний інститут (Massachusetts Institute of Technology); 3. Каліфорнійський університет в Берклі (University of California – Berkley); 4. Університет Карнегі (Carnegie Mellon University); 5. Корнелл університет (Cornell University); 6. Пристонський університет (Princeton University); 7. Техаський університет (University of Texas at Austin); 8. Іллінойський університет (University of Illinois at Urbana-Champaign); 9. Вашингтонський університет (University of Washington); 10. Університет Вісконсін-Медісон (University of Wisconsin-Madison).

Технічне оснащення університетів США активно підтримують різні інвестори. Зокрема, «Палац комп'ютерних наук» і лабораторія з комп'ютерних систем Стенфордського університету (режим доступу до веб-сторінки: <http://www.stanford.edu/>) були побудовані за фінансової допомоги Білла Гейтса – співзасновника і генерального директор фірми Microsoft, який пожертвував на будівництво майже 6 млн. доларів. Приміщення обладнані сучасною комп'ютерною і комунікаційною технікою, теле- і відеопроєкційним устаткуванням, програмними засобами на основі багатьох платформ операційних систем. Центральний вхід у цей «Палац» названий на честь жертводавця.

Школа менеджменту Krannert Університету Пурду (Purdue University – <http://www.mgmt>) штату Індіана вдячна фірмам IBM, Hewlett-Packard, Sap America за допомогу у створенні її комп'ютерного лабораторного комплексу. Лабораторії, бібліотека і комп'ютерні класи школи завдяки об'єднанню в мережу Інтернет, стали доступними не тільки викладачам і студентам, які перебувають на території ВНЗ, а й тим, хто вчиться на далекій відстані від нього. Студенти, використовуючи систему інтегрованих курсів навчання Katalyst, мають доступ до розкладу занять, дискусійних груп, домашніх завдань, веб-сторінок викладачів тощо.

Вивчаючи професійну підготовку фахівців в галузі інформаційної безпеки в американських ВНЗ, ми визначали мету нашого дослідження у контексті таких критеріїв: цілі навчання; зміст професійної підготовки із захисту інформації та принципи його відбору; методи і форми такої підготовки.

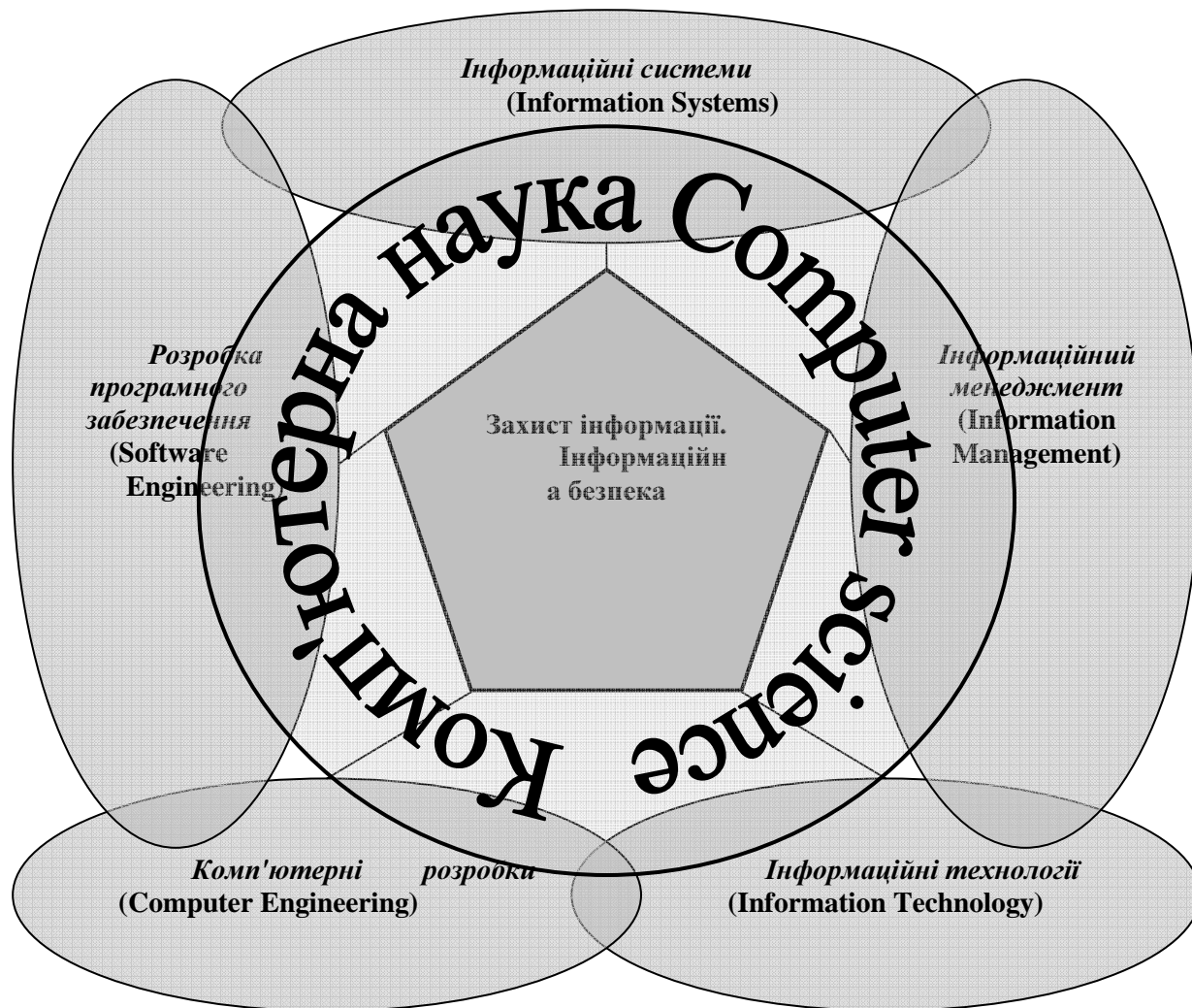


Рис. 1. Види професійної діяльності фахівця із захисту інформації та управління інформаційною безпекою у США та інших розвинутих країнах Заходу.

Вище зазначалося, що фахівців із захисту інформації та управління інформаційною безпекою в зарубіжних ВНЗ готують у рамках названих напрямів. Найбільший пласт спеціальностей і спеціалізацій, пов'язаних із захистом інформації, знаходиться в рамках напрямку Computer Science. Так, наприклад, на факультеті комп'ютерних наук Йельського університету (Computer science Yale University – <http://www.cs.yale.edu/>) готують фахівців у галузі захисту інформації на рівні магістрів з криптографії і комп'ютерної безпеки (спеціальність COS 467). Бакалаврський рівень освіти цієї спеціальності можна одержати в коледжі при цьому університеті.

Йельські дослідницькі програми коледжу пропонують студентам комплекс навчальних дисциплін, пов'язаних з комп'ютерними науками. Перелічимо їх: Вступ до програмування, Графічний користувальницький інтерфейс; Використання комп'ютерної графіки; Математичні інструменти в інформатиці; Від піктограми до пікселя; шлях людської комунікації; Структури даних і методи програмування; Системне програмування і комп'ютерна організація; Цифрові логічні пристрої; Компілятори і перекладачі; Операційні системи; Теорія розподілених систем; Безпека на засадах мовних середовищ; Функціональне програмування; Формальна семантика; Основи комп'ютерної музики; Комп'ютерні мережі; Мобільні технології і безпроводна організація мережі; Мережні вилучені системи і датчики; Вступ до бази даних; Програмування систем бази даних; Комп'ютерні системи; Числові обчислювальні методи; Вступ до пошуку даних; Економічна інформатика; Особиста інформація і її захист; Основи криптографії; Графи і мережі; Математичне програмування; Криптографія і комп'ютерна безпека; Теорія складних систем; Інтелектуальна робототехніка; Комп'ютерна графіка; Комп'ютерне моделювання і

мультиплікації; Цільові комп'ютерні курси; Спеціальні проекти. Серед представлених навчальних дисциплін понад 30% безпосередньо пов'язані з проблемами захисту інформації, а ті, що залишилися, – опосередковано.

Специфіка підготовки фахівців із захисту інформації та управління інформаційною безпекою у США потребує від випускників коледжів та університетів міждисциплінарної підготовки. Студентів уже не задовольняє жодна дисципліна, жодна спеціальність у «чистому» вигляді. Міждисциплінарний принцип підготовки таких фахівців є одним з провідних у ВНЗ цієї країни. Навчальні програми підготовки насичені інтегрованими дисциплінами, спрямованими на професійну підготовку. В Йельському університеті студентам пропонують такі «interdisciplinary» та «multidisciplinary» курси: Нові прогресивні ідеї в інформатиці; Інформатика і сучасна інтелектуальна підготовка; Інтернет: еволюційні технології і суспільство; Цифровий фотореалізм; Комп'ютери і закон; Таємність у цифровому столітті; Інтелектуальна власність у цифровому столітті; Проектний і алгоритмічний аналіз; Філософія програмування; Паралельні методи програмування; Доказове програмування; Генна інженерія і біоінформатика; Цифрова відеотехніка на основі біосистем; Нейронні мережі в обчислювальній техніці; Штучні нейронні мережі; Штучний інтелект. Отже, студенти не лише набувають суто професійних знань, умінь і навичок прикладного характеру, у них формуються професійно-значущі якості – комунікабельність, толерантність, уміння працювати з людьми, гнучко мислити, творчо оцінювати ситуацію, керувати колективом [5, с. 142].

Департамент інформатики (Department of Computer Science) Принстонського університету (<http://www.princeton.edu/main/>) був біля створення першої в світі обчислювальної техніки, починаючи з Алана Тюринга і Джона фон Неймана, які були його співробітниками. За останні кілька років відділ пережив істотні зміни і тепер має 30 факультетів з потужними дослідницькими групами в галузі комп'ютерної теорії, інформаційних систем, графічних оболонок, мов програмування, обчислювальної техніки, інформаційної безпеки, штучного інтелекту й обчислювальної біології. На факультеті інформатики готують, зокрема фахівців зі спеціальності «Захист інформації» (COS 432: Information Security).

У рамках напряму *Information technology* розвивається підготовка фахівців у сфері захисту інформації, яка сфокусована на використанні інформаційних технологій. Так, в Університеті Пурду (<http://www.purdue.edu/>) є програма Secure Purdue, спрямована на вивчення й удосконалення мережної безпеки інформації. Серед семи газузей, які охоплює ця програма, головною складовою є та, що займається вивченням шляхів безпеки інформації за допомогою комп'ютерних технологій. Є також галузі, де досліджуються проблеми захисту інформації з позиції законності, а також з позиції методичних проблем підготовки кадрів для кожної галузі. Наукові розробки сприяють підвищенню безпеки даних в Інтернеті, збереженню особистісного інформаційного захисту і недоторканості приватного життя не тільки для тих, хто знаходиться в середовищі Purdue, а й тих, хто, навчаючись за цією програмою, буде захищати особистісну конфіденційну інформацію своїх клієнтів.

У Массачусетському технологічному інституті (<http://web.mit.edu/>) є спеціальність «Мережі і комп'ютерна безпека» (IT 6.857: Network and Computer Security), у рамках якої студенти вивчають багато дисциплін. Профілюючими серед них є такі: Методи безпеки в багатокористувацьких і розподілених комп'ютерних системах; Криптографія: секретний ключ, суспільно-значущі цифрові підписи; встановлення дійсності документів і схеми ідентифікації; Виявлення вручання та віруси; Формальні моделі комп'ютерної безпеки; Безпечні операційні системи; Захист програмного забезпечення; Безпека електронної пошти та інформації у Всесвітній павутині; Електронна торгівля: протоколи оплати, електронні гроші; Брандмауери; Оцінка ризиків.

Декан факультету інженерії та прикладних наук Принстонського університету, професор електротехніки Майкл Генрі Стрейтер, розповідаючи про свій факультет, вказує, що основним напрямком науково-дослідної діяльності при підготовці фахівців електротехніки, які пов'язані із захистом інформації в комунікаційних мережах, є такий напрям, що відстежує досягнення високої пропускну здатності каналів зв'язку при передаванні інформації. Він зауважує: «Наші фахівці мають глибокі знання з методології використання безпроводних комунікаційних мереж, завдяки чому можуть з великою вірогідністю виявляти не тільки пропускну здатність каналів зв'язку, а й затримки, що можливі у разі несанкціонованого доступу до каналу в мережі» [6].

Наукова школа підготовки таких фахівців базується на використанні передових дидактичних розробок, на основі статистичних методів обробки інформаційних сигналів, а також на базі впровадженні ефективних датчиків для реєстрації сторонніх підключень. Така підготовка фахівців в галузі інформаційної безпеки вписується у напрям підготовки Computer Engineering.

Зазначимо, що в департаменті комп'ютерних наук (Department of Computer Science) Принстонського університету студенти навчаються на іншій спеціальності – «Захист інформації» (COS 432: Information Security), яка належить до напрямку *Computer Science*.

Якщо подивитися на розподіл годин, що виділяються на вивчення дисципліни у ВНЗ нашої країни і цього університету, то можна побачити явно виражений контраст. У документах державного стандарту України кількість часу, що надається для аудиторних занять, становить більшу частку – 70%, на самостійну роботу студентів – 29–28% і лише 1-2% на контроль здобутих знань та придбаних умінь. Критерії для атестації студентів Принстонського університету визначаються наступним співвідношенням навчальної підготовки: 70% – домашня робота, 20% – заключний іспит, 10% – аудиторні заняття. Отже, основна форма праці, під час якої американська студенти одержують знання та вміння їх використовувати, – це самостійна робота без залучення допомоги викладача. Значне місце в навчальному процесі надається контролю за виконанням навчальної програми і відповідності набутих знань до вимог освітнянського стандарту.

Лабораторія «Мережної безпеки» (Network Security Lab) кафедри інформатики Колумбійського університету (<http://nsl.cs.columbia.edu/>) займається виконанням передових наукових досліджень у найважливіших сферах захисту інформації в комп'ютерних мережах і створення систем мережної безпеки. Ці дослідження містять у собі нові методи ефективного кодування інформації; розробку систем мережної надійності, систем управління інформаційною безпекою і розгалужених систем швидкого реагування; безпеку розподілених систем. Також займаються проблемами несанкціонованого доступу до інформації і виявленням мережного втручання до таємної інформації, проводять аналіз аномалій при передачі даних у мережах, займаються питаннями загальної політики мережної безпеки і доступу до даних. Студенти й аспіранти беруть участь у перерахованих проектах, удосконалюють свої навички в практичній діяльності, вивчають спеціалізовані науково-дослідні теми і виконують конкретні роботи в галузі мережної безпеки. В університеті виходить безкоштовний щомісячний електронний бюлетень «Crypto-Gram», який висвітлює питання комп'ютерної безпеки у використанні електронної пошти і прикладних аспектах криптографії. Цей напрям підготовки майбутніх фахівців функціонує в рамках двох напрямів – Information Systems і Computer Science.

Із 90-х років XX ст. у США та інших розвинених країнах менеджмент використовує нове покоління інформаційних технологій. Від створення інформації (нових знань), її передання, переробки – до використання, щоб перетворити і захистити об'єкти, де вона відтворюється, а також захистити саму себе – ось неповний перелік замкнутого інформаційного циклу. Інформаційні технології цього рівня передбачають вищий етап комп'ютеризації інформаційного менеджменту – Information Management. У цьому випадку людина з її творчими здібностями органічно прилучається до автоматизованої системи переробки і використання інформації.

Аналізуючи розвиток професіоналізму майбутніх фахівців у сфері інформаційної безпеки в США, можна зробити висновки, що він нерозривно пов'язаний із індивідуалізацією навчання. У більшості ВНЗ не існує поняття академічної групи, академічного курсу, фіксованого терміну навчання. Студент фактично має змогу формувати індивідуальний освітній модуль відповідно до особистих інтересів та уявлень про майбутню кар'єру. Викладачі-наставники допомагають студентові скласти таку індивідуальну програму навчання, щоб вона дала змогу реалізувати його внутрішнє покликання до тієї чи іншої науково-дослідницької теми. Майбутній фахівець навчається по індивідуальній траєкторії, з урахуванням розподілу свого фізичного і розумового навантаження, з обліком власної комфортності.

## ЛІТЕРАТУРА

1. Постанова Кабінету Міністрів України від 13 грудня 2006 р. № 1719 «Перелік напрямів, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційним рівнем бакалавра». Ст. 3333. // Офіційний вісник КМ України від 25.12.2006 р. – № 50. – С. 160.

2. Computing Curricula 2005. The Overview Report. – A volume of the Computing Curricula Series. – A cooperative project of the ACM, the AIS, the IEEE-CS. 30 September 2005. – 55 p.
3. Абасова С. Э. Подготовка специалистов в области информационной безопасности [Электронный ресурс] / Судаба Эйбалы кызы Абасова // Институт информационных технологий Национальной Академии наук Азербайджана. – Режим доступа: [www.science.az](http://www.science.az) – Заголовок з екрана.
4. Маклаков Г. Научно-методологические аспекты подготовки специалистов в области информационной безопасности / Центр исследования компьютерной преступности. 28.01.2005 // Режим доступа: <http://www.crime-research.ru>. – Заголовок з екрана.
5. Коваль Т. І. Теоретичні та методичні основи професійної підготовки з інформаційних технологій майбутніх менеджерів-економістів: Дис. ... д-ра пед. наук: 13.00.04 / Тамара Іванівна Коваль – К., 2008. – 574 с.
6. Strater M.H. University Professor of Electrical Engineering [Электронный ресурс] / Michael Henry Strater // Princeton University, Department Electrical Engineering. Режим доступа: <http://www.princeton.edu/main/facstaff/.htm> – Заголовок з екрана.