**УДК 378.147:004.056.5**
**EL 378.147:004.056.5**

**Сергій Володимирович МЕЛЬНИК**

кандидат технічних наук, доцент, докторант
«Національна академія Служби безпеки України»

**Сергій Олегович ВОСКОБОЙНІКОВ**

кандидат педагогічних наук, старший викладач
«Національна академія Служби безпеки України»

e-mail: G_Vosk@ukr.net

# ОСОБЛИВОСТІ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ В КІБЕРПРОСТОРІ В СПОЛУЧЕНИХ ШТАТАХ АМЕРИКИ

***Анотація**. У статті розглядаються особливості професійної підготовки фахівців із захисту інформації в кіберпросторі на прикладі провідних вищих навчальних закладів США. Узагальнюється тематичне наповнення навчального процесу із сучасної підготовки бакалаврів і магістрів із захисту інформації. Визначено, що в межах неперервного навчання розглядаються напрями реалізації професійної кар'єри: інженерів із захисту інформації; менеджерів та аудиторів систем захисту інформації; аналітиків і консультантів із захисту інформації.*
***Ключові слова:** професійна підготовка, захист інформації, інформаційна безпека, IT- безпека, комп'ютерна і мережева безпека.*

**Вступ.** Сучасні тенденції забезпечення академічної мобільності у вищій освіті надають можливість студентам, аспірантам і науково-педагогічному складу вищих навчальних закладів брати участь у різноманітних навчальних або навчально-дослідницьких програмах, що сприяє підвищенню якості освіти, розвитку міжкультурного обміну, інтеграції у світовий науково-освітній простір. В умовах реформування вищої освіти України фактор академічної мобільності є одним із пріоритетів при започаткуванні професійної підготовки майбутніх фахівців з інформаційної і кібернетичної безпеки.

Сучасна галузь діяльності із забезпечення інформаційної і кібернетичної безпеки включає в себе правовий, організаційний, технічний і правоохоронний складники, стосується інформаційно-технологічного та інформаційно-психологічного протиборства. При цьому основна частина сучасного ринку праці визначається потребами у фахівцях з технічного і криптографічного захисту інформації у кіберпросторі (далі – захисту інформації).

Терміни «технічний» і «криптографічний захист інформації» є нормативно закріпленими та широко вживаними у професійному середовищі пострадянського простору. У Сполучених Штатах Америки та країнах Європейського Союзу застосовуються такі терміни, як «інформаційна безпека (information security)» у розумінні захисту інформації, «кібербезпека (cyber security)», «IT-безпека (IT security)», «комп'ютерна і мережева безпека (computer and network security)», «комп'ютерні системи безпеки (computer system security)», «інформаційні системи безпеки (information system security)»,

«електромагнітна інформаційна безпека (electromagnetic information security)», «фізична інформаційна безпека (physical information security)», «менеджмент інформаційної безпеки (information security management)», «криптографія (cryptography)» та інші.

Розглядаючи захист інформації як складник інформаційної безпеки, зосередимо увагу на тому, що в нормативно закріплених термінах в Україні, сучасна діяльність із захисту інформації передбачає розгляд:

– правових питань визначення необхідності та порядку захисту інформації, правового супроводу етапів розробки, упровадження, експлуатації та виведення з експлуатації систем захисту;

– технологічних питань захисту інформації в інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності;

– організаційних і технічних питань управління інформаційною безпекою (а точніше, управління захистом інформації).

Отже, з урахуванням суспільної необхідності та соціального замовлення на підготовку майбутніх фахівців із захисту інформації, а також сутності професійної діяльності, розглянемо зазначену проблему.

**Аналіз досліджень і публікацій.** Професійна підготовка за напрямом «Кібербезпека» в університетах США поєднує теорію і ноу-хау з оцінки, планування, проектування та реалізації ефективних заходів кіберзахисту в державному та приватному секторах, орієнтована на кар'єру фахівців з цифрової (комп'ютерної, IT) криміналістики, аналітиків і консультантів з кібербезпеки. Програми підготовки відповідають вимогам директиви 8570.01-M Міністерства оборони США [4–6] і цілям Міжнародної асоціації фахівців з комп'ютерних розслідувань (IACIS) [7].

Питання професійної підготовки майбутніх фахівців із захисту інформації у США розглядали вітчизняні фахівці В. Артемов, Ю. Даник, М. Коляда, В. Остроухов, Ю. Супрунов та ін. Однак враховуючи високі темпи розвитку сучасних ІТ технологій, методів і засобів їх захисту, що обумовлюють нові вимоги до професійних компетенцій та професійної компетентності майбутніх фахівців, доцільно розглянути сучасний досвід професійної підготовки фахівців із захисту інформації у США [9–11].

**Мета:** визначення змістового наповнення професійної підготовки майбутніх фахівців із захисту інформації в кіберпросторі у вищих навчальних закладах США.

**Завдання:**

- дослідження особливостей бакалаврської і магістерської професійної підготовки майбутніх фахівців із захисту інформації, а також тематичного наповнення навчального процесу з питань захисту інформації в інформаційно-телекомунікаційних системах, управління захистом інформації та кібербезпеки.

Наукова новизна полягає в тому, що вперше здійснено системний аналіз особливості професійної підготовки майбутніх фахівців із захисту інформації в кіберпросторі в Сполучених Штатах Америки та здійснено впровадження передового досвіду в освітній процес підготовки майбутніх фахівців кібербезпеки.

**Результати досліджень.** Узагальнюючи результати дослідження компетентнісного підходу ВНЗ США, можна виділити основну особливість – «гнучкість» навчального процесу, орієнтованого на досягнення успіху кожного студента у формуванні професійної компетентності, доступності вищої освіти, зокрема. Ця «гнучкість» полягає у формуванні особистого навчального плану, тобто графіка вивчення навчальних дисциплін з урахуванням особистих інтелектуальних можливостей, результатів попереднього

навчання, наявного досвіду, професійних схильностей та уподобань. При цьому кількість нормативних дисциплін у провідних вищих навчальних закладах значно менша порівняно з навчальними дисциплінами за вибором студентів, що дозволяє кожній особистості ефективніше планувати власну систему навчання й професійного розвитку та неперервного навчання впродовж життя.

Крім того, у вищих навчальних закладах реалізується схема індивідуального наставництва (Student Mentor) – допомога закріпленої до студента контактної особи у плануванні та корекції організації навчання за індивідуальною траєкторією, з урахуванням результатів профорієнтації та побажань студента щодо розподілу свого фізичного і розумового навантаження – забезпечення власної комфортності під час навчання.

Апробованою часом інновацією є також он-лайн навчання (e-learning) фахівців із захисту інформації в межах бакалаврської та магістерської програм, а також післядипломної освіти. Вочевидь он-лайн навчання лише в комплексі з окресленими особливостями компетентнісного й особистісно орієнтованого підходів надає підстави для реального підвищення доступності якісної освіти для майбутніх і діючих фахівців із захисту інформації та професійного розвитку.

Підготовка бакалавра «Інформаційні технології – безпека (Information Technology – Security)» та магістра «Кібербезпека інформаційного забезпечення (Cybersecurity and Information Assurance)» здійснюється у Західному губернаторському університеті (Western Governors University), єдиному в історії вищої освіти США університеті, що акредитований у чотирьох регіональних комісіях з акредитації. Онлайн університет заснований у 1997 році 19 губернаторами у місті Солт-Лейк-Сіті штату Юта.

Напрям підготовки «Інформаційних технології – безпека» освітньо-кваліфікаційного рівня (ОКР) «Бакалавр» передбачає формування професійної компетентності з управління інформаційною безпекою, забезпечує можливості для отримання студентами сертифікатів Cisco Certifications, CIW Certifications, CompTIA Certifications, (ISC)2 Certifications, Microsoft Certifications, Project Management Institute Certifications, Oracle/Java Certifications, GIAC Certifications, IBM Certifications [2]. Програма призначена перш за все для здобувачів вищої освіти, які вже мають певний рівень технічних знань: штатних менеджерів з IT-безпеки; досвідчених IT-спеціалістів, які мають бажання перейти в IT-безпеку; для всіх студентів, які мають 15 і більше годин на тиждень на онлайн навчання. Назви основних тематичних напрямів професійної підготовки: «програмування», «операційні системи», «управління даними», «бізнес інформаційних технологій», «мережева безпека та безпека даних».

Магістерська підготовка за напрямом «Кібербезпека інформаційного забезпечення» орієнтована на майбутніх фахівців з цифрової економіки приватного сектору, що володіють ключовими компетентностями відповідно до національної ініціативи США 2014 року для освіти з кібербезпеки (NICE) Workforce Framework [3]. Основними тематичними напрямами дисциплін професійної підготовки є: «управління ризиками», «кібервійни», «нормативно-правове забезпечення кібербезпеки», «політика безпеки», «безпека апаратного і програмного забезпечення», «етичний хакінг», «криміналістика мережевих вторгнень (комп'ютерна або IT криміналістика)», «аварійне відновлення, запобігання та реагування».

Особливістю онлайн навчання у Західному губернаторському університеті є підтвердження компетентностей у рамках розробленої системи оцінювання та перенесення кредитів. Тобто якщо студент уже володіє певними компетентностями і здатен це підтвердити, то він може не втрачати час та матеріальні ресурси на вивчення відповідних дисциплін. Для кожного студента прикріплюється наставник (студентський куратор), який допомагає йому реалізувати особистісно орієнтоване навчання та поточну допомогу в якісному засвоєнні професійної компетентності.

У Американському військовому університеті (American Military University) готують бакалаврів «Безпека інформаційних систем (Information Systems Security)» та «Кібербезпека (cybersecurity)», магістрів «Кібербезпека (cybersecurity)», «Національна безпека (National Security)» та «Внутрішня безпека (Homeland Security)» – онлайн освіта для військовослужбовців, ветеранів та цивільних осіб [4]. Крім того, проводиться онлайн навчання та сертифікація фахівців, що уже мають досвід роботи.

Підготовка бакалавра за напрямом «Безпека інформаційних систем» в Американському військовому університеті поєднує теорію з технічними навичками забезпечення інформаційної безпеки (захисту інформації) підприємств, державних установ і військових формувань, спрямована на формування кар'єри майбутніх менеджерів з інформаційної безпеки, аналітиків, аудиторів, консультантів та експертів з управління ризиками. Дисципліни цієї програми відповідають вимогам директиви 8570.01-M [5] Міністерства оборони США та окремі дисципліни, сертифіковані за сприяння Агентства національної безпеки (NSA) Information Assurance Courseware Evaluation (IACE) [6]. Основними тематичними напрямами дисциплін професійної підготовки є

«комп'ютерна та мережева безпека», «захист операційних систем», «мережеві атаки, кіберзлочинність, кіберзаконодавство», «управління ризиками інформаційної безпеки», «забезпечення неперервності бізнесу та відновлення після збоїв», «аудит безпеки IT, планування та політика», «кіберзаконодавство та недоторканність приватного життя в епоху цифрових технологій», «цифрова (комп'ютерна, IT) криміналістика».

Підготовка бакалавра за напрямом «Кібербезпека» в Американському військовому університеті поєднує теорію і ноу-хау з оцінки, планування, проектування та реалізації ефективних заходів кіберзахисту в державному та приватному секторах, орієнтована на кар'єру фахівців з цифрової (комп'ютерної, IT) криміналістики, аналітиків і консультантів з кібербезпеки. Дисципліни цієї програми відповідають цілям Міжнародної асоціації фахівців з комп'ютерних розслідувань (IACIS) [7] і вимогам директиви 8570.01-M Міністерства оборони США. Основними тематичними напрямами дисциплін професійної підготовки є «кіберзлочинність, кібербезпека, кібервійни», «біометрія, криптографія і фізичний захист», «захист операційних систем», «цифрова криміналістика і розслідування мережевих вторгнень», «кримінологія, розвідка і національна безпека», «безпровідний та мобільний зв'язок», «інформаційне забезпечення та IT-безпека», «кіберзаконодавство, етика і конфіденційність в епоху цифрових технологій».

Підготовка магістра «Кібербезпека» в Американському військовому університеті передбачає використання широкого міждисциплінарного підходу до запобігання і реагування на масштабні кіберзагрози і кібератаки. Перша половина програми навчання включає основи мережевої безпеки, кіберзлочинності та цифрової криміналістики. У другій половині програми основна увага приділяється

політиці, практиці і перспективам забезпечення кібербезпеки в межах заходів національної безпеки, розвідки, кримінального правосуддя й управління надзвичайними ситуаціями. Основними тематичними напрямами дисциплін професійної підготовки є «перспективи управління в надзвичайних ситуаціях і кібербезпека», «управління ризиками безпеки методами запобігання втрат», «історія, розвиток і ефективність кіберрозвідки», «комп'ютерна (цифрова, IT) криміналістика: інструменти, процедури та законодавство», «профілактика і розслідування кіберзлочинів», «телекомунікації та мережева безпека: запобігання, виявлення та реагування на інциденти», «кіберзакони, етика, інтелектуальна власність і кримінальне переслідування».

Магістратура «Національна безпека» та «Внутрішня безпека» передбачає розгляд окремих питань інформаційної безпеки в межах комплексного підходу до забезпечення національної і внутрішньої безпеки.

Особливість он-лайн навчання в Американському військовому університеті полягає в комплексному підході до професійної підготовки фахівців з інформаційної і кібернетичної безпеки державного і приватного секторів у розрізі забезпечення громадської, внутрішньої, національної та міжнародної безпеки, а також використання державних і громадських програм доступу до вищої освіти військовослужбовців і ветеранів (безкоштовне навчання або знижки на отримання освітніх послуг для військовослужбовців, ветеранів і студентів, що вирішили підписати контракт з Міністерством оборони (DOD), Агентством національної безпеки (NSA) та Агентством внутрішньої безпеки (DHS) США).

У Католицькому університеті Льюіс (Lewis University) штат Іллінойс готують бакалаврів «Інформаційна безпека і

управління ризиками (Information Security and Risk Management)» та магістрів «Інформаційна безпека (Information security)».

Підготовка бакалавра за напрямом «Інформаційна безпека і управління ризиками» у Католицькому університеті Льюіс поєднує в собі надання технічних знань з теорією управління, глибоким концептуальним розумінням основ інформаційної безпеки, управління ризиками, управління безпекою, IT-операцій і передачі даних, комп'ютерної (цифрової, IT) експертизи, етичного хакінгу. Основними тематичними напрямами дисциплін професійної підготовки є: «управління мережевою безпекою», «практика управління безпекою», «криптографія», «архітектура і моделі безпеки», «безпека IT-операцій», «забезпечення неперервності бізнесу та аварійного відновлення», «IT-законодавство та етика», «фізична інформаційна безпека», «комп'ютерна (цифрова, IT) криміналістика».

Підготовка магістра за напрямом «Інформаційна безпека» у Католицькому університеті Льюіс зорієнтована на формування теоретичного і практичного складника професійної компетентності майбутніх фахівців із захисту інформації, що включають два тематичні блоки: технічна концентрація (призначений для IT-фахівців, що відповідають за виявлення порушень у системі безпеки, реалізацію рішень з дотримання політик і процедур безпеки); управлінська концентрація (призначений для IT-керівників, менеджерів з інформаційної безпеки, а також директорів, які відповідають за проектування і підтримку IT-інфраструктури та системи менеджменту інформаційної безпеки). Загальними тематичними напрямами дисциплін професійної підготовки є «архітектура комп'ютерних систем: апаратний і програмний складники», «основи програмування (C ++, Java і PHP)», «вступ до

інформаційної безпеки (розроблення плану і політики безпеки, управління ризиками, володіння технологіями PGP, SSH і SCP)», «безпека мереж передачі даних (фізичний, канальний, мережевий і транспортний рівень моделі OSI)», «виявлення, реагування та відновлення після мережевих вторгнень», «шифрування та автентифікація», «правові та етичні проблеми інформаційної безпеки».

Особливість організації навчання студентів у Католицькому університеті Льюіс полягає в організації он-лайн навчання з особистим наставником для отримання освітніх ступенів «бакалавр» і «магістр», а також підготовки до сертифікації CompTIA Security+, Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), AccessData Certified Forensics Examiner (ACE). Університет має державне замовлення силових відомств США – DOD, NSA та DHS.

Отже, на основі здійсненого аналізу можна систематизувати тематичне наповнення бакалаврської програми майбутніх фахівців із захисту інформації, що складається, насамперед, з таких професійних орієнтацій як: «архітектура і моделі безпеки»; «безпека даних»; «безпека IT-операцій»; «захист операційних систем»; «комп'ютерна безпека»; «мережева безпека»; «управління мережевою безпекою»; «криптографія»; «фізична інформаційна безпека»; «управління ризиками інформаційної безпеки»; «забезпечення неперервності бізнесу та відновлення після збоїв»; «аудит інформаційної безпеки»; «IT-законодавство та етика»; «кіберзаконодавство та недоторканність приватного життя в епоху цифрових технологій». У свою чергу, тематичне наповнення магістерської програми майбутніх фахівців із захисту інформації включає передусім компетентності з

розроблення політик безпеки, розроблення та експлуатації технологій захисту на різних рівнях моделі OSI, обробки інцидентів інформаційної безпеки.

Окремо зазначимо, що ґрунтовний правовий та економічний складник професійної компетентності із захисту інформації формується окремими дисциплінами або спеціалізаціями в межах магістратури з правових і економічних наук [9].

**Висновки.** Результати дослідження свідчать, що у вищій освіті США наявні спеціальності як з інформаційної безпеки (у розумінні захисту інформації), так і кібербезпеки. При цьому різниця в змістовому наповненні між ними достатньо умовна. Особливість спеціальності кібербезпека полягає, насамперед, у технічному складнику військової сфери та правоохоронної діяльності: кібервійни – національна безпека; протидія кіберзлочинності – громадська, національна і міжнародна безпека; захист критичної інформаційної інфраструктури – внутрішня безпека.

Провідні вищі навчальні заклади США готують: інженерів із захисту інформації (розробників, системних адміністраторів та ін.); менеджерів та аудиторів з технічних або організаційно-правових, організаційно-технічних та економічних спеціалізацій з управління захистом інформації; аналітиків і консультантів із захисту інформації; правознавців та економістів за спеціалізацією інформаційна (кібер) безпека. Навчальний процес передбачає формування таких професійно-значущих якостей особистості, як комунікабельність, толерантність, уміння працювати з людьми, гнучко мислити, творчо оцінювати ситуацію, управляти ризиками.

Основним координатором з питань професійної підготовки фахівців з інформаційної і кібернетичної безпеки є АНБ, яке тісно співпрацює з іншими

структурними підрозділами МО США, а також з МВБ, ЦРУ, ФБР, НАСА, Міністерством фінансів, Мін'юстом, Міненерго.

**Перспективами подальшого розвитку напряму досліджень** є вивчення досвіду професійної підготовки фахівців із захисту інформації країн Європейського Союзу.

## ЛІТЕРАТУРА


1. Western Governors University official site [Електронний ресурс]. – Режим доступу : http://www.wgu.edu (дата звернення: 30.11.2016).
2. Western Governors University certifications [Електронний ресурс]. – Режим доступу : http://www.wgu.edu/admissions/it_certifications (дата звернення: 30.11.2016).
3. NICE official site [Електронний ресурс]. - Режим доступу : http://csrc.nist.gov/nice/framework (дата звернення: 30.11.2016).
4. American Military University official site [Електронний ресурс]. – Режим доступу : https://www.amu.apus.edu (дата звернення: 30.11.2016).
5. Information Assurance Workforce Improvement Program Department of Defense instruction DoD 8570.01-M [Електронний ресурс]. – Режим доступу : http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf (дата звернення: 30.11.2016).
6. Information Assurance and Security Education Center official site [Електронний ресурс]. – Режим доступу : https://iasec.eller.arizona.edu/programs/iace-courseware (дата звернення: 30.11.2016).
7. International Association of Computer Investigative Specialists (IACIS) official site [Електронний ресурс] – Режим доступу : http://www.iacis.com (дата звернення: 30.11.2016).

8. Albany Law School official site [Електронний ресурс] – Режим доступу : http://www.albanylaw.edu/academic-life/degrees/master-of-science-in-legal-studies/cybersecurity-and-data-privacy (дата звернення: 30.11.2016).
9. Чванова М.С. Подготовка кадров в области информационной безопасности в США / М. С. Чванова, М. Анурьева // Вестник ТГУ. - 2012. - №8 - С. 126-133.
10. Коляда М.Г. Підготовка фахівців із захисту інформації та управління інформаційною безпекою в країнах Європейського Союзу / М.Г. Коляда // Проблеми сучасної педагогічної освіти : зб. статей ; вип. 25. – Ч. 2. – Ялта : КГУ, 2010. – Ч. 2. – С. 72–75. – Серія «Педагогіка. Психологія»
11. Даник Ю.Г. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України / Ю.Г. Даник, Ю.М. Супрунов // Збірник наукових праць ЖВІ НАУ «Інформаційні системи» ; випуск 5. - 2011. - С. 5-22

**Транслітераційний переклад використаних джерел**

1. Western Governors University official site [Електронний ресурс]. – Режим доступу : http://www.wgu.edu (30.11.2016).
2. Western Governors University certifications [Електронний ресурс]. – Режим доступу : http://www.wgu.edu/admissions/it_certifications (: 30.11.2016).
3. NICE official site [Електронний ресурс]. - Режим доступу : http://csrc.nist.gov/nice/framework (30.11.2016).
4. American Military University official site [Електронний ресурс]. – Режим доступу : https://www.amu.apus.edu (30.11.2016).
5. Information Assurance Workforce Improvement Program Department of Defense instruction DoD 8570.01-M [Електронний ресурс]. – Режим доступу :

http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf (дата звернення: 30.11.2016).
6. Information Assurance and Security Education Center official site [Електронний ресурс] – Режим доступу : https://iasec.eller.arizona.edu/programs/iace-courseware (30.11.2016).
7. International Association of Computer Investigative Specialists (IACIS) official site [Електронний ресурс]. – Режим доступу : http://www.iacis.com (30.11.2016).
8. Albany Law School official site [Електронний ресурс] – Режим доступу : http://www.albanylaw.edu/academic-life/degrees/master-of-science-in-legal-studies/cybersecurity-and-data-privacy (дата звернення: 30.11.2016).
9. Chvanova M. S. Podhotovka kadrov v oblasti ynformatsyonnoy bezopasnosti v SShA / M. S. Chvanova, M. Anur'eva // Vestnyk THU. 2012. #8 S.126-133.
10. Kolyada M. H. Pidhotovka fakhivtsiv iz zakhystu informatsiyi ta upravlinnya informatsiynoyu bezpekoyu v krayinakh Yevropeys'koho soyuzu / M. H. Kolyada // Problemy suchasnoyi pedahohichnoyi osvity. Seriya «Pedahohika. Psykholohiya» : zb. statey. – Yalta : K·HU, 2010. – Vyp. 25. – Ch. 2. – S. 72–75.
11. Danyk Yu. H. Deyaki pidkhody do formuvannya systemy pidhotovky kadriv dlya systemy kibernetychnoyi bezpeky Ukrainy / Yu. H. Danyk, Yu. M. Suprunov // Zbirnyk naukovykh prats' ZhVI NAU «Informatsiyni systemy». Vypusk 5. 2011. S.5-22

**Serhii MELNYK**

Candidate of Technical Sciences, Associate professor, doctoral candidate
«National Academy of Security Service of Ukraine»

**Serhii VOSKOBOINIKOV**

Candidate of pedagogical sciences, Senior Lecturer,
«National Academy of Security Service of Ukraine»

e-mail: G_Vosk@ukr.net

## PECULIARITICS OF PROFESSIONAL TRAINING OF SPECIALISTS IN THE US CYBERSPACE INFORMATION PROTECTION

***ABSTRACT.*** *The article considers the features of professional training of specialists for the information protection in cyberspace at the example of some leading universities in the United States of America. The thematic content of the learning process for the preparation of modern bachelors and masters of information security has been summarized.*

*Building on systematic analysis, it has been found that training in "cyber security" in the United States combines theory and know-how of evaluation, planning, design and implementation of effective measures in public and private sectors cyber focused on career professionals in digital (computer, IT) forensic analysts and consultants on cyber security.*

*Modern sector activities for providing information and cyber security includes legal, organizational, technical and law enforcement components of the concerns of information technology and information-psychological confrontation. The*

*modern labor market determines the need for specialists in technical and cryptographic protection of information in cyberspace.*

*The leading US universities prepare: Data Protection Engineers (developers, system administrators etc) managers and auditors of technical, legal, organizational and economic specializations of information security management, analysts and consultants of information security; lawyers and economists with specialization «Information (cyber) security». Educational process involves the formation of professionally significant personality qualities: communication, tolerance, ability to work with people, think flexibly and creatively, assess the situation to manage risks.*

*In the framework of lifelong learning the areas of implementation of engineers professional career of in information protection, management and auditing of information security system; analysts and consultants on information security have been considered.*
***Key words**: professional training, information protection, information security, IT security, computer and network security.*

**Сергей Владимирович МЕЛЬНИК**

кандидат технических наук, доцент, докторант
«Национальная академия Службы безопасности Украины»

**Сергей Олегович ВОСКОБОЙНИКОВ**

кандидат педагогических наук, старший преподаватель
«Национальная академия Службы безопасности Украины»

e-mail: G_Vosk@ukr.net

# ОСОБЕННОСТИ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ В КИБЕРПРОСТРАНСТВЕ В США

***Аннотация.*** *В статье рассматриваются особенности подготовки специалистов по защите информации в киберпространстве на примере ведущих высших учебных заведений США. Обобщается тематическое наполнение учебного процесса современной подготовки бакалавров и магистров по защите информации. Установлено, что в рамках непрерывного образования рассматриваются направления реализации профессиональной карьеры: инженеров по защите информации; менеджеров и аудиторов систем защиты информации; аналитиков и консультантов по защите информации.*

***Ключевые слова:*** *профессиональная подготовка, защита информации, информационная безопасность, ИТ-безопасность, компьютерная и сетевая безопасность.*