4 Підготовка, перепідготовка та підвищення кваліфікації спеціалістів системи захисту інформації

УДК 638.253. 231.

ПІДГОТОВКА ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПІДРОЗДІЛІВ ОРГАНІВ ВНУТРІШНІХ СПРАВ

Микола Браіловський, Володимир Хорошко
Національний авіаційний університет України

Анотація: **Сформульовано і визначено шляхи ефективного вирішення задачі підготовки фахівців із захисту інформації в Україні.**
Summary: **In work are formulated and the ways of the effective decision of a task of preparation of the experts on protection of the information in Ukraine are determined.**
Ключові слова: **Захист інформації, підготовка фахівців, технічний захист інформації.**

І Вступ

Система підготовки та перепідготовки фахівців із захисту інформації, яка склалася у другій половині 70-х років, сьогодні переживає нову трансформацію і модернізацію з урахуванням сучасних вимог, що висуваються до захисту інформації і, як наслідок, до рівня підготовки фахівця.

Питання про підготовку, перепідготовку та підвищення кваліфікації фахівців із захисту інформації (ЗІ) вперше було поставлено у другій половині 60-х років. Тоді воно розглядалося тільки в площині кадрового забезпечення захисту державних секретів, оскільки комерційної таємниці в СРСР не існувало, а захист несекретної інформації не був настільки актуальним, як сьогодні.

Хоча обсяг державних секретів України у порівнянні з обсягами за часів СРСР у деякій мірі знизився, проте він продовжує залишатися значним у найважливіших сферах діяльності держави. Про це свідчать Закони України "Про інформацію", "Про державну таємницю" та інші нормативні документи. Обсяг інформації, що захищається, не скоротився, оскільки в Україні, в силу її геополітичного положення, військового та економічного потенціалу, зберігається велика кількість інформації про політичні, військові, економічні, науково-технічні та інші сектори інтересів держави. Така інформація потребує надійного захисту, бо її витік до потенційного супротивника здатний викликати політичні ускладнення, ослаблення військової та економічної потужності країни.

Разом з тим поряд з продовженням існування державної таємниці з'явилась і комерційна таємниця. В міру зростання кількості підприємств недержавного сектора збільшується і обсяг інформації, що складає комерційну таємницю. Від надійності захисту цієї інформації залежить ефективність функціонування комерційних підприємств, їх безпека і конкурентоспроможність.

Відповідно до нього в нинішній час під концепцією інформаційного забезпечення діяльності будь-якого об'єкту розуміється вирішення трьох макрозадач:

- формування і поточне корегування інформаційного кадастру об'єкту, вибір джерел інформації для регулярного поповнення і відновлення його;
- поточне відновлення, поповнення і функціональне використання інформаційного кадастру об'єкту відповідно до мети функціонування об'єкту;
- відслідковування відповідності вхідного потоку інформації стану інформаційного кадастру об'єкту та меті функціонування об'єкту і прийняття необхідних рішень і заходів при неузгодженості значень перерахованих параметрів.

Тому з розширенням застосування при обробці інформації засобів обчислювальної техніки можливості втрати такої інформації різко зростають.

Ускладнення відбувається і за рахунок перегляду принципів засекречування інформації, модифікації правових основ захисту її [1 – 2, 4].

Що стосується захисту комерційної таємниці, то тут діє ряд специфічних обставин, що впливають на організацію її захисту. На комерційних підприємствах ЗІ є прерогативою самих підприємств. Об'єкти комерційної таємниці встановлюють і видозмінюють індивідуально, на рівні їх власників, відповідно до норм права, виробничих, торговельних і фінансових процедур, укладених угод, спрямування інтересів

конкурентів, споживчої цінності і т. д. [3]. У таких умовах важливе значення мають характер і джерела комерційної таємниці, її носії, градації за ступенем захищеності, специфічні канали витоку інформації і т. д.

II Основна частина

Зростання можливостей щодо несанкціонованого одержання інформації, розширення за рахунок появи нових конкурентів "контингенту" організацій і осіб, зацікавлених у несанкціонованому одержанні інформації, поява додаткових каналів витоку інформації, передусім у процесі обробки інформації засобами електронно-обчислювальної техніки, використання нових методів і засобів несанкціонованого одержання інформації значно ускладнили умови ЗІ, особливо в частині протидії технічній розвідці та попередження несанкціонованої модифікації інформації в АСОД шляхом зараження її вірусами і програмними закладками різних видів і типів.

Забезпечення режиму інформаційної безпеки в умовах, що постійно змінюються і ускладнюються, вимагає постійного проведення:

- фундаментальних та прикладних досліджень явищ і процесів у даній предметній області,
- необхідної кількості підготовлених і компетентних фахівців.

Критичний погляд на питання державної політики підготовки кадрів із інформаційної безпеки наведено в [5]. Можна цілком погодитись з тим, що в нових умовах ситуація з забезпеченості кадрами у сфері ЗІ не може бути визнана задовільною і потребує реорганізації. Ця проблема ще підсилюється і тим, що:

- різко зменшилося фінансування освіти;
- з'явилася небезпека розвалу існуючої системи підготовки кадрів; можливість втрати науково-методичного та професійно-викладацького потенціалу, а також матеріально-технічної бази;
- відсутній системний підхід з програмно-цільовим плануванням і оптимальним розподілом ресурсів,
- відсутня планова політика в питаннях підготовки фахівців з ЗІ та у справах інформаційної безпеки.

Рекомендації Постанови Кабінету Міністрів України, нещодавніх конференцій та семінарів, присвячених проблемі підготовки кадрів із ЗІ [6 – 8] , зводяться до:

- збільшення чисельності фахівців, оскільки їх кількість не задовольняє існуючим потребам;
- безперервного вдосконалення навчального процесу з метою підготовки висококваліфікованих фахівців, оскільки теорія і практика ЗІ безперервно та інтенсивно розвиваються і нові досягнення мають якнайшвидше знайти відображення у навчальних планах і програмах;
- розширення номенклатури спеціальностей із ЗІ, оскільки сучасні системи забезпечення інформаційної безпеки стають все більш складними і комплексними як за метою, так і за методами і засобами, що використовуються.

Наслідком цього процесу і стала поява певної модифікації та тенденції у системі підготовки та підвищення кваліфікації фахівців із ЗІ.

Таким чином, саме життя ставить наступні довгострокові цілі у цій області:

1) підготовка та перепідготовка фахівців, здатних ефективно вирішувати сучасні задачі ЗІ в Україні;
2) збільшення чисельності фахівців, які проходять підготовку та перепідготовку за напрямком ЗІ;
3) об'єднання зусиль провідних освітніх і наукових колективів та адміністративних органів для вирішення масштабних практичних проблем ЗІ;
4) створення та постійний розвиток регіональних наукових шкіл в області інформаційної безпеки;
5) створення умов для забезпечення режиму інформаційної безпеки держави в цілому, регіонів, підприємств та окремих громадян.

До короткострокових задач, на наш погляд слід віднести:

- створення та освоєння освітнього процесу за напрямком інформаційної безпеки в Україні;
- проведення наукових досліджень і формування на базі провідних вищих навчальних закладів (ВНЗ) та академічних інститутів регіональних наукових об'єднань, здатних у майбутньому об'єднати широке коло дослідників для вирішення крупномасштабних задач інформаційної безпеки;
- ефективне використання регіональних інформаційних баз, наукових центрів та обладнання для навчання та проведення практичних занять студентів, аспірантів та фахівців, які проходять перепідготовку, з проблем забезпечення ЗІ, для проведення НДР викладачів ВНЗ та співробітників центрів перепідготовки фахівців із ЗІ;
- вирішення спільно з регіональними адміністративними органами конкретних практичних задач в області інформаційної безпеки.

Слід відзначити, що деякі з цих короткострокових задач сьогодні вже вирішуються. Так з 1998 року працює Міжгалузевий міжрегіональний семінар Національної Ради НАН України "Технічні засоби захисту інформації", який має відділення в Києві при Національному авіаційному університеті, у Львові при Національному університеті "Львівська політехніка", у Харкові при Харківському технічному університеті

радіоелектроніки, у Дніпропетровську при Національній гірничий академії України та при Дніпропетровському державному університеті.

Як бачимо охоплені західні, північні, центральні та східні регіони України. Зараз створюється ще три відділення у місті Одесі на базі Одеського філіалу Української академії державного управління при Президентові України, у місті Вінниці у Державному технічному університеті, та у Севастополі на базі Військово-морського інституту.

З цього видно, що регіональні відділення Семінару можуть стати об'єднуючим ядром для вирішення як короткострокових, так і довгострокових задач у напрямку інформаційної безпеки.

Не претендуючи на оригінальність та враховуючи все зазначене, автори бачать такі шляхи вирішення проблеми підготовки фахівців за напрямком ЗІ [6, 10]:

1) удосконалення знань у процесі навчально-виховної підготовки у відповідних областях математики, фізики, інформатики та інших дисциплін таких як: функціональний аналіз, теорія розпізнавання образів, нейромережеві алгоритми, сучасні методи цифрової обробки сигналів та інші;

2) поетапна постановка лабораторних та практичних занять на наявній у ВНЗ як звичайній, так і спеціальній апаратурі, а також залучення до проведення лабораторних та практичних занять фахівців зацікавлених міністерств та відомств з технікою, яка знаходиться у них на озброєнні;

3) науково-дослідна робота студентів та слухачів під час навчального процесу.

Наразі в загальному переліку спеціальностей вищої освіти, затвердженому Постановою № 507 Кабінету Міністрів України від 24.05.97 (зі змінами від 18.06.98), існують лише два напрямки підготовки фахівців, безпосередньо пов'язаних з інформаційною безпекою держави.

Однак, широкий аспект забезпечення інформаційної безпеки держави задовільнений на даний час лише деякими напрямками, пов'язаними з так званим технічним аспектом безпеки інформації: 0924 "Телекомунікації" та 1601 "Інформаційна безпека". Зовсім не розкриті в існуючому переліку спеціальностей напрями:

- підготовки фахівців в нормативно-правовому аспекті забезпечення безпеки інформаційного простору держави (тобто забезпечення юриспруденції при протидії засобам інформаційної боротьби в системах мас-медіа, усунення причин інформаційної дискримінації держави та ін.);

- підготовки фахівців в галузі гуманітарного забезпечення безпеки інформаційного простору держави (тобто забезпечення філософських аспектів формування громадянського суспільства в умовах інтенсивного розвитку інформаційної сфери, безпечної інтеграції України у світове інформаційне співробітництво);

- підготовки фахівців в галузі кібернетично-інформаційної протидії (тобто застосування сучасних засобів інформаційної зброї, включаючи програмні продукти та апаратні засоби, інформаційні технології інших держав) тощо.

В період існування СРСР підготовка кадрів в області захисту державних секретів і протидії технічним розвідкам була зосереджена в невеликій кількості спеціалізованих цивільних та військових вищих навчальних закладів, де навчався ретельно відібраний контингент студентів чи слухачів.

Однак структурно-змістовна перебудова вищої освіти в державі, яка почалася на початку 90-х років, з'ясування українськими ВНЗ за два-три останніх роки конкурентоспроможності спеціальностей в області інформаційної безпеки зумовили початок підготовки таких фахівців в різноманітних навчальних закладах України.

Це, по-перше. введення у перелік ліцензованих спеціальностей вищої освіти: 7.092482 – безпека інформації в спеціалізованих інформаційних системах; 7.160101 – захист інформації з обмеженим доступом та автоматизація її обробки (в комп'ютерних системах); 7.160102 – ахист інформації з обмеженим доступом та автоматизація її обробки; 7.160103 – системи захисту від несанкціонованого доступу; 7.160104 – адміністративний менеджмент в системах захисту інформації з обмеженим доступом; 7.160105 – захист інформації в комп'ютерних системах та мережах.

Однак потрібно визнати, що підготовка фахівців із інформаційної безпеки завжди мала індивідуальну спрямованість, не була "масовою" чи поставленою "на потік". Це дозволяло згуртувати в окремо визначених державою ВНЗ відповідних фахівців, вчених та методистів найвищого рівня підготовки, які істотно вплинули на коло професійних ознак студентів після випуску з ВНЗ.

Підготовка фахівців має ґрунтуватися на системному підході, що дозволяє структурувати і порівнювати різні технічні, природничо-наукові та інші фахи і спеціалізації в області інформаційної безпеки залежно від того, за яким призначенням будуть в майбутньому працювати випускники. Фахівці мають проходити підготовку за технічним і природничо-науковим профілем, як вузьким так і широким. Дотепер у рамках Міністерства освіти і науки України недостатньо пророблена номенклатура спеціальностей в області інформаційної безпеки з позиції аналізу сфер, видів, об'єктів, методів і засобів професійної діяльності в цій галузі. При цьому необхідно враховувати існуючий дефіцит науково-педагогічних кадрів для ВНЗ і науково-

дослідних закладів. Задача підготовки висококваліфікованих фахівців має вирішуватися в рамках системи підготовки, перепідготовки і підвищення кваліфікації в області інформаційної безпеки та захисту інформації, що в даний час в Україні лише формується. Система, що відображає специфічні риси предметної сфери, має розглядатися як складова частина загальнодержавної системи підготовки, перепідготовки і підвищення кваліфікації кадрів.

Особливості проблеми захисту інформації пред'являють певні специфічні вимоги до студентів і, відповідно, до навчального процесу.

Насамперед, як показує досвід підготовки фахівців з інформаційної безпеки та захисту інформації, необхідно приділити особливу увагу доборові студентів і при цьому враховувати їхні індивідуально-психологічні особливості, риси характеру, технічну підготовку і загальну культуру.

З метою створення повноцінної та ефективної системи підготовки кадрів у напрямку інформаційної безпеки починаючи з 1995 року, коли було підписано спільний наказ Державної служби України з питань технічного захисту інформації та Міністерства освіти України від 28.12.1995 № 66/358 "Про співробітництво між Міністерством освіти України та Державною службою України з питань технічного ЗІ".

Подальшим кроком у проведенні державної політики щодо підготовки та підвищення кваліфікації фахівців в області ЗІ стала Постанова Кабінету Міністрів України від 8 жовтня 1997 року №1126 "Про концепцію технічного захисту інформації в Україні". Згідно з цією Постановою [6] у розділі 4 записано "Першочерговими заходами щодо реалізації державної політики у сфері ТЗІ є: ... визначення реальних потреб системи Т31 у фахівцях, розвиток та вдосконалення системи підготовки, перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ".

Для виконання положень Постанови та спільного наміру Міністерства освіти і науки України та Служби безпеки України від 23.08.2000 року № 404 створено, як відокремлений структурний підрозділ Національного авіаційного університету, Інститут інформаційно-діагностичних систем. В зв'язку з цим змінився підхід до підготовки фахівців у галузі захисту інформації. В Інституті об'єднані спеціальності за напрямком 1601 "Інформаційна безпека": 7.160102, 7.160103 та 7.160105. Підготовка студентів проводиться на кафедрах: інформаційно-вимірювальних систем, засобів захисту інформації та комп'ютеризованих систем захисту інформації. Така робота проводиться з кандидатами протягом двох років їх підготовки в Інституті і лише на третьому курсі після тестування і співбесіди, де враховуються всі перераховані вище якості, вони зараховуються до навчальної групи. При цьому недостатня увага до людського чинника часто являє собою більш значну загрозу, чим використання новітніх технічних засобів для здобування секретної інформації. Поняття "людський чинник" містить у собі особисті якості, що виражають цілісну характеристику особистості, її відмінність від інших людей. На думку фахівців, незважаючи на різноманітність та "витонченість" спеціальної техніки для одержання бажаної інформації, люди залишаються одним із самих ймовірних джерел витоку інформації. Саме людина виступає основою будь-якої інформації. При підборі кандидатів, яким треба буде працювати із секретною інформацією, необхідно враховувати їх ділові, професійні, моральні якості та психологічні особливості. Тут важливо скласти уявлення не тільки про окремі якості і риси кандидата, а також про особистість у цілому, її світоглядних установках, інтелекті, переконаннях, ціннісних орієнтаціях, здібностей до даного виду діяльності, рисах характеру і т. п. Необхідно формувати та виховувати і студентів пильність, обов'язковість, особисту відповідальність за виконання доручених завдань.

При формуванні навчального плану необхідно передбачити підготовку майбутніх фахівців, залежно від спеціальності, за якою здійснюється підготовка, також в області чинного законодавства, криптографічного і технічного захисту, організаційних і фізичних заходів захисту, а також в області психології, моралі й етики. Підготовка в такій області як психологія не менш важлива, ніж в інших. Адже уміння визначити психологічний тип співрозмовника і правильно провести бесіду багато в чому визначає ефективність визначення наявності або відсутності каналів витому інформації.

У зв'язку з цим у Національному авіаційному університеті, якому Міністерством освіти і науки України доручено очолити розробку освітнього стандарту з напрямку підготовки "Інформаційна безпека" 1601, розроблено навчальні плани підготовки фахівців із ЗІ. Вони, в цілому, мають забезпечити загальноосвітню та спеціальну підготовку фахівців. Розроблений навчальний план підготовки кадрів із ЗІ також спрямовано на підготовку фахівців-універсалів, які володіють методами, обізнані на засобах та технологіях захисту інформації, що складає будь-який вид таємниці, які володіють правовими, організаційними, програмно-математичними та інженерно-технічними основами ЗІ, та які здатні організувати і забезпечити комплексну систему ЗІ. Однак незабаром стало ясно, що в умовах розширення видів таємниці, ускладнення задач із ЗІ, збільшення обсягу загально гуманітарних дисциплін необхідна для підготовки багатопрофільних фахівців кількість годин не вкладається у рамки навчального плану. Тому, було прийнято рішення здійснювати підготовку фахівців даного напрямку за трьома спеціальностями: 7.160102 -"Захист інформації з обмеженим

доступом та автоматизація її обробки", 7.160103 – "Системи захисту від несанкціонованого доступу" та 7,160105 – "Захист інформації в комп'ютерних системах та мережах". У рамках спеціальності 7.160103 підготовка здійснюється за двома спеціалізаціями: 7.160103.01 – системи внутрішньо об'єктового контролю та 7.160103.02 - системи захисту інформації від витоку технічними каналами.

Проведення в життя цього рішення проходило двома етапами. У 1998 році були складені навчальні плани для цих спеціальностей, які врахували всі перераховані особливості, та почали впроваджуватись в навчальному процесі. В 2000 році після проведення корегування цих планів за ними почали навчатися студенти 1 курсу. Студенти 5 – 6 курсів продовжують навчатися за старим навчальним планом, а для студентів 2 – 4 курсів було розроблено "перехідні", комбіновані робочі та навчальні плани.

Крім того слід враховувати, що підготовка фахівців ведеться як за державним замовленням, так і на контрактній основі. Це обумовлює, що частина фахівців в подальшому буде працювати в державних структурах, а частина – в недержавних.

У зв'язку з цим необхідно розширити рамки і чисельність контингенту підготовки фахівців із захисту інформації. Воно повинно відбуватися за рахунок введення в різноманітних навчальних закладах спеціалізацій, пов'язаних із безпекою інформації. Це в першу чергу відноситься до економістів, юристів, медиків і т. д.

Складніше організувати підготовку фахівців середньої ланки, необхідність в яких, на наш погляд, має тенденцію до зростання. Це питання мабуть слід вирішувати за рахунок бакалаврів, підготовлених у вищих навчальних закладах.

Диференціювання у певній мірі вже знайшло практичне втілення. Так, в результаті проведених консультацій та обговорювань, в тому числі за участю фахівців інших вузів та зацікавлених міністерств і відомств, було вироблено наступні підходи [7 – 8]:

- при збереженні однакових сфер та об'єктів професійної діяльності мають бути зазначені відмінності за видами професійної діяльності, оскільки вони впливають на характер знань та вмінь фахівця;
- має бути визначений склад базових дисциплін, які необхідні для кожної спеціальності;
- необхідно посилити і диференціювати загально професійну підготовку фахівців за кожною спеціалізацією;
- склад і зміст спеціальних дисциплін за кожною спеціалізацією мають охоплювати інформацію, що складає всі види таємниці, розкривати всі види, методи, засоби та технологію ЗІ, однак, при цьому необхідно враховувати специфіку професійної діяльності випускника;
- прийом кандидатів на навчання повинен здійснюватися не за спеціальностями та спеціалізаціями, а в загальний бакалаврат у цілому, розподіл студентів за спеціальностями та спеціалізаціями має здійснюватися за їхнім бажанням і на основі конкурсного відбору наприкінці 4-го семестру, коли вибір кваліфікації вже є усвідомленим, до безпосереднього розподілу за спеціальностями навчання має бути спільним за всіма дисциплінами, після розподілу – за співпадаючими;
- після розподілу за спеціальностями і спеціалізаціями студентам протягом наступних 4-х семестрів має бути надано право на зміну спеціальності або спеціалізації за умови "доздачі" дисциплін за новою спеціалізацією, що не вивчалися або вивчалися в меншому обсязі з колишньої спеціальності.

З урахуванням цих підходів розроблено державний освітній стандарт з підготовки фахівців за освітнім напрямком 1601 "Інформаційна безпека".

III Висновки

Необхідно звернути увагу на підвищення вимог до якості підготовки фахівців. Поява нових каналів витоку інформації та засобів її несанкціонованого одержання, необхідність забезпечення надійної безпеки, зростаюча вартість інформації поставили питання про навчання фахівців не тільки традиційним методам та засобам ЗІ, але і новим підходам та навичкам в області попередження витоку інформації, її несанкціонованого копіювання, модифікації, блокування, знищення, інших незаконних форм втручання в інформаційні ресурси та системи. Та й традиційні методи та засоби ЗІ вимагають вдосконалення і "прив'язки" до умов, що змінюються.

Більше того, сучасний фахівець із ЗІ повинен уміти визначати склад інформації, що захищається, її цінність, ступінь вразливості, розраховувати шкоду від можливої втрати інформації, оцінювати якість і ефективність різноманітних методів та засобів захисту, проводити спеціальні дослідження і сертифікацію різноманітних технічних засобів обробки і ЗІ, орієнтуватися на вітчизняному та зарубіжному ринку засобів ЗІ, проектувати та впроваджувати системи ЗІ, знати та використати зарубіжний досвід.

Впровадження технічних засобів обробки інформації, в першу чергу комп'ютерних, вимагає від фахівців уміння вільного користування ними, а входження українських підприємств в світову економіку, створення спільних підприємств – різкого збільшення обсягу знань іноземних мов.

Все це тягне за собою суттєве корегування навчальних планів і програм.

У загальну систему підготовки кадрів з інформаційної безпеки входить не тільки освітня первинна підготовка відповідних фахівців у ВНЗ, але й додаткова наукова підготовка, основне місце в якій належить підготовці науково-педагогічних кадрів в аспірантурі і докторантурі.

*Література: **1**. Закон України "Про державну таємницю". **2**. Закон України "Про інформацію". **3**. ДСТУ 3396.0-96 Технічний захист інформації. Основні положення. **4**. Звід відомостей, що становлять державну таємницю № 52 від 01.03.2001 р. **5**. Лазарєв Г. П., Кльоцкін С. М., Хорошко В. О. Шляхи вирішення проблеми інформаційної безпеки в Україні. // Захист інформації, 2000, № 2. – с. 4 – 9. **6**. Постанова Кабінету Міністрів України від 8.10.1997 р. №1126 "Концепція технічного захисту інформації в Україні". **7**. Збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – К.: НТУУ "КПІ", 2001 р. **8**. Материалы IV Международной научно-технической конференции "Безопасность информации в информационно-телекомуникационных системах". – К.: ДСТСЗИ, 2001 г.*

УДК 638.253.231

ОСВІТНЬО-КВАЛІФІКАЦІЙНА ХАРАКТЕРИСТИКА ФАХІВЦЯ З ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ. ДОСВІД ЄВРОПЕЙСЬКОГО УНІВЕРСИТЕТУ

Андрій Гринь
Європейський університет

Анотація: **Наведені погляди щодо змісту освіти підготовки фахівців з організації захисту інформації з обмеженим доступом.**
Summary: **The content of grounding in organization of information with restricted access.**
Ключові слова: **Організація захисту, інформація з обмеженим доступом, управління.**

Розвиток економіки України зумовив необхідність підготовки фахівців з організації захисту інформації з обмеженим доступом для сфери підприємницької діяльності. В основному сформувалося правове поле захисту комерційної таємниці. Але зміст підготовки фахівців у даній, дуже важливій галузі не в повному обсязі відповідає вимогам часу стосовно бізнес-структур.

Орієнтуючись саме на недержавний сектор економіки держави, спираючись та керуючись принципами забезпечення національної безпеки держави на основі вивчення та узагальнення потреб та замовлень підприємців, було запропоновано новітній підхід до підготовки фахівців з організації захисту інформації з обмеженим доступом в рамках спеціальності 160104 “Адміністративний менеджмент в системах захисту інформації з обмеженим доступом”. Основні принципи викладені в освітньо-кваліфікаційній характеристиці (ОКХ) випускника Європейського університету. В даному документі узагальнюється зміст освіти, тобто відображаються цілі освітньої та професійної підготовки, визначаються місце спеціаліста з фаху “Адміністративний менеджмент в системах захисту інформації з обмеженим доступом” у структурі господарства держави та вимоги до його компетентності, інших соціально важливих властивостей та якостей.

Цей документ є складовою частиною системи стандартів вищої освіти, в якій узагальнюються вимоги до змісту освіти та навчання з боку держави та споживачів випускників Європейського університету. ОКХ відображає соціальне замовлення на фахівця у сферах праці та професійної підготовки з урахуванням аналізу професійної діяльності.

ОКХ використовується при:

- визначенні первинних посад випускників Європейського університету та умов їх використання;
- визначенні цілей освітньої та професійної підготовки;
- розробленні та корегуванні освітньо-професійної програми підготовки спеціалістів з фаху “Адміністративний менеджмент в системах захисту інформації з обмеженим доступом”;
- розробленні засобів діагностики рівня якості освітньо-професійної підготовки спеціаліста;
- визначенні змісту навчання як бази для оволодіння новими спеціальностями, кваліфікаціями;
- визначенні змісту навчання у системі перепідготовки та підвищення кваліфікації;
- атестації випускників Європейського університету та сертифікації фахівців;
- укладанні договорів або контрактів щодо підготовки фахівців;