УДК 004.056.5.378.1

В.Л. Бурячок, І.Р. Пархомей,
М.М. Степанов, В.Б.Толубко

ПРОБЛЕМНІ ПИТАННЯ ТА АКТУАЛЬНІ ЗАВДАННЯ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ГАЛУЗІ ЗНАНЬ «ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ»

Розвиток інформаційних та комунікаційних технологій спричинив глибокі системні перетворення в інформаційному та кібернетичному просторах. Останній, в силу своєї специфіки, породжує нові загрози та виклики фахівцям з інформаційної безпеки. Традиційні фахівці з інформаційної безпеки зіштовхуються з новими специфічними завданнями, які вимагають від них нових знань та вмінь. З огляду на це, у роботі, для забезпечення потреб силових структур, а також виробничої та банківської сфери України у фахівцях, спроможних виявляти ознаки та активно протидіяти сторонньому кібернетичному впливу, авторами пропонується підхід до запровадження в системі вищої освіти України профілю навчання «кібернетична безпека». Крім того, чітко визначено критерії,яким мають відповідати такі фахівці.

Ключові слова: інформаційно-комунікаційні технології, інформаційна безпека, інформаційний простір, кібернетичний простір, кіберзагроза, кібероперації, кібербезпека, підготовка фахівців.

Вступ і постановка задачі

Інформаційно-комунікаційні технології (ІКТ) стали нині потужною силою перетворення суспільного життя та інноваційного розвитку. Їх активне впровадження практично в усі сфери життєдіяльності міжнародної спільноти змінило останнім часом світову економіку й спричинило глибокі системні перетворення в глобальному інформаційному та кібернетичному просторах.

Маючи певну специфіку, ці глобальні субстанції породжують, в свою чергу, нові й, передусім, кібернетичні загрози і виклики, розв'язувати які мають фахівці з інформаційної безпеки (ІБ), озброєні новими знаннями і вміннями та інноваційними підходами. Зважаючи на таке саме питання забезпечення безпеки цих субстанцій в умовах ведення, провідними країнами світу міждержавного протиборства й, перш за все, забезпечення їх інформаційної та кібернетичної безпеки, як головних складових національних безпекових систем та підготовки фахівців, спроможних це зробити, набувають нині особливої гостроти і актуальності [1 – 4].

Виклад основного матеріалу досліджень

Надзвичайно загостреною ця проблема постає останнім часом. Цьому сприяє, перш за все, вибухове зростання обсягів інформації, до яких отримали доступ пересічні громадяни, винайдення потужних комп'ютерів і вбудованих мікроконтролерів, що привело переважну більшість країн світу як до глобальної інтелектуалізації та гіпершвидкого розвитку промисловості, так й зробило більш вразливими до загроз антропогенного і техногенного характеру, а також природних катаклізмів, передусім, критично-важливі сегменти та об'єкти їх економіки. На це значною мірою впливає той факт, що нині більш затребуваним стає не захист інформації як такої, а забезпечення безпеки, власне, тієї інформаційно-комунікаційної системи (ІКС), на вхід якої ця інформація потрапляє, де вона циркулює, накопичується та обробляється.

Зробити такий висновок спонукають [5 – 9]:

по-перше, вимоги сьогодення щодо усвідомлення таких понять, як кіберпростір, під яким переважна частина фахівців у галузі ІБ та захисту інформації розуміють віртуальне соціотехнічне середовище із завданнями програмного забезпеченням комп'ютерної техніки, мережевого та телекомунікаційного обладнання, так і кібербезпека, під якою ті ж фахівці вбачають складову частину поняття інформаційної безпеки (розглядає ті ж самі загрози, методи, засоби і заходи захисту, але лише в просторі кібернетичному);

по-друге, вимоги міжнародного стандарту ISO/IEC 27032:2012(E), який виражає погляд на ці питання міжнародного експертного середовища й регламентує кібербезпеку окремим доменом безпеки, що забезпечує конфіденційність, цілісність і доступність інформації у кіберпросторі та має прояви лише у взаємодії людей і організацій в Інтернет;

по-третє, вимоги затверджених Указами Президента України Стратегії національної безпеки України та Стратегії кібербезпеки України, в яких пріоритетами забезпечення національної безпеки визначено, зокрема, удосконалення професійної підготовки у сфері інформаційної безпеки, створення системи підготовки кадрів у сфері кібербезпеки для

потреб органів сектору безпеки і оборони та залучення наукових установ, навчальних закладів, тощо до розробки та реалізації заходів із кібербезпеки і кіберзахисту.

В умовах України, як на наш погляд, одною із головних проблем залишається при цьому саме незадовільне кадрове забезпечення фахівцями із кіберзахисту. Про таке свідчать матеріали аналітичної доповіді Національного інституту стратегічних досліджень при Президентові України «Кібербезпека: світові тенденції та виклики для України», а також результати аудиту нещодавно виведених з обігу стандартів вищої освіти у галузі знань 1701 «Інформаційна безпека», які показали, що професійні компетентності, задекларовані в цих галузевих стандартах, неповною мірою враховують стан та перспективу розвитку методів і засобів забезпечення кібербезпеки.

Імовірно, саме це стало відправною точкою для прийняття постанови Кабінету Міністрів України від 29 квітня 2015 року №266, яка внесла зміни до «Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» та визначила для України лише одну безпекову спеціальність – 125 «кібербезпека», імплементація якої в освітній процес дасть змогу сформувати базис у виді компетентностей (соціально-особистісних, інструментальних, загальнонаукових, професійних тощо), виробничих функцій (дослідницьких, проектувальницьких, організаційних, управлінських, технологічних, контрольних, прогностичних, технічних тощо) та типових задач, що ним відповідають, а також умінь, якими мають володіти випускники й фактично закласти фундамент для їх практичної роботи за напрямом організації та забезпечення кібернетичної безпеки.

Виходячи з цього та з врахуванням вимог Закону України «Про вищу освіту» стають актуальними питання щодо змісту, обсягу та оцінювання якості змісту і результатів освітньої діяльності ВНЗ за спеціальністю «кібербезпека» [4] (розроблення стандарту вищої освіти), запровадження спеціалізацій, що відповідають спеціальностям колишньої галузі знань «інформаційна безпека», розроблення нових освітніх програм та проведення їх акредитації. Формування професійної компетентності майбутніх фахівців кібернетичної безпеки розглядається при цьому, як трирівневий педагогічний процес, який відповідно до вимог закону України «Про вищу освіту» включає послідовну й неперервну фахову підготовку відповідно до Галузевих стандартів вищої освіти на першому (бакалаврському) і другому (магістерському) освітньо-професійних та третьому (доктор філософії) освітньо-науковому рівнях й здійснюється у вищих навчальних закладах III – IV рівнів акредитації або у спеціалізованих структурних підрозділах – навчально-наукових інститутах. Формування спеціальних професійних якостей, необхідних для реалізації фахових компетенцій майбутніх фахівців кібербезпеки (табл. 1), здійснюється у процесі професійної підготовки – вивчення спеціальних навчальних дисциплін за освітньою та навчальною складовими відповідно до профілей освітньо-наукових програм та відповідних стандартів вищої освіти нового покоління, які мають формуватися на основі компетентнісного підходу.

Таблиця 1

Загальні та професійні компетентності фахівця із «кібербезпеки»

	Програмні компетентності				
1	Загальні		2	Професійні	
	Шифр	Зміст		Шифр	Зміст
	ЗК-1	**Уміння критичної самооцінки** – здатність визначати та задовольняти потреби особистого та наукового розвитку, бути критичним і самокритичним.		ПК-1	**Інтегративнакомпетентність** – здатність до інтеграції знань, умінь і навичок та їх ефективного використання в умовах швидкої адаптації організацій до вимог зовнішнього середовищ, що забезпечують виконання завдань науково-дослідної, науково-педагогічної, управлінської та інноваційної діяльності в інформаційній та безпековій сферітощо.
	ЗК-2	**Навички творчого спілкування** – здатність спілкуватися результативно в усній і письмовій формах з фахівцями та нефахівцями, здатність спілкуватися другою мовою.		ПК-2	**Соціально-психологічна компетентність** (емоційні, перцептивні, концептуальні, поведінкові) – здатність особистості орієнтуватися у різних життєвих ситуаціях, ефективно працювати в умовах ринкової економіки; уміння реалізувати стратегії і плани; здатність до розуміння поведінки людей, мотивації та організації їх спільної діяльності тощо.
	ЗК-3	**Знання інформаційних технологій** – здатність використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах.		ПК-3	**Організаційно-комунікативна компетентність** (у специфічних сферах управлінської діяльності) – здатність до лідерства та новаторської діяльності, до формування високого рівня комунікативної культури; здатність переконувати оточуючих, стверджувати свою позицію; володіння державною мовою, грамотним усним та писемним діловим мовленням, ораторським мистецтвом, професійним етикетом, а також
	ЗК-4	**Навички керування проектами** – здатність демонструвати своєчасність та плановість у дослідженні, здатність до адаптації та дії в новій ситуації, здатність розробляти та управляти проектами.			

	ЗК-4	**Навички керування проектами** – здатність демонструвати своєчасність та плановість у дослідженні, здатність до адаптації та дії в новій ситуації, здатність розробляти та управляти проектами.			навичками публічної презентації результатів роботи, вміннями обирати відповідні форми і методи презентації; володіння іноземними мовами, уміння правильно розмовляти та писати різними комунікативними стилями, а саме неофіційним, офіційним та науковим тощо.
	ЗК-5	**Уміння підтримати інших** – здатність допомагати через викладання, наставництво та наочні приклади (демонстрацію).		ПК-4	**Професійна компетентність** – теоретична та практична підготовленість фахівця, що забезпечує ефективність вирішення професійних проблем і типових професійних завдань; стан володінняІТ та технологіями захисту інформації; здатність до удосконалення та впровадження у практику інновацій у сфері інформаційної та кібербезпеки; ступінь використання наукової літератури та інших джерел інформації для реалізації інноваційних технологій; здатність до здійснення ефективного пошукута структурування інформації,до кваліфікованої роботи з різними ІР тощо.
	ЗК-6	**Уміння працювати етично** – здатність визначати, поважати та керувати етичними, культурними та іншими питаннями, пов'язаними з наявністю тих чи інших відмінностей.		ПК-5	**Загальнонаукова компетентність** – здатність до накопичення професійних вмінь та навичок (діагностування й інтерпретування ситуацій, планування та здійснення наукових досліджень, викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційних технологій та захисту інформації); здатність до генерування нових знань з теорії захисту інформації та інформаційної безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки; здатність до застосування нових знань у професійній діяльності (проектній, винахідницькій та раціоналізаторській роботі) тощо.
	ЗК-7	**Навички підприємництва** – здатність визначати підприємницькі можливості чи вид діяльності або громадського впливу, здатність приймати обґрунтовані рішення, здатність оцінювати та забезпечувати якість виконуваних робіт.		ПК-6	**Політехнічна компетентність** – знання загальних (методологічних, історичних, економічних, ергономічних тощо) питань безпекової сфери, принципів дії і будови основних функціональних органів інформаційних систем; здатність до оволодіння спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та без пековими технологіями; здатність до застосування різноманітних, професійно профільованих знань і практичних навичок у сфері захисту інформації.
	ЗК-8	**Уміння командної роботи** – знання про стимули та бар'єри в ефективній командній роботі, вміння виявляти, ставити та вирішувати проблеми.		ПК-7	**Інженерна компетентність** – здатність до виробничо-технологічної діяльності (розробки та впровадження інноваційних технологій ІБ, вибору технології ІБ, устаткування та засобів, використання ІТ; розробки програм і методик випробувань систем інформаційної та кібербезпеки); здатність до організаційно-управлінської діяльності (організації процесу створення та надання інфокомунікаційних послуг); здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки ІКС, до обробки та перетворення інформації тощо.
		За проектом TUNING. *1. Здатність до абстрактного мислення, аналізу та синтезу.* *2. Здатність застосовувати знання у практичних ситуаціях.* *3. Знання та розуміння предметної області та розуміння професії.* *4. Здатність спілкуватися другою мовою.* *5. Навички використання інформаційних і комунікаційних технологій.* *6. Здатність вчитися і бути сучасно навченим.* *7. Здатність бути критичним і самокритичним.* *8. Здатність до адаптації та дії в новій ситуації.* *9. Вміння виявляти, ставити та вирішувати проблеми.* *10. Здатність приймати обґрунтовані рішення.* *11. Здатність працювати в команді.* *12. Здатність мотивувати людей та рухатися до спільної мети.* *13. Здатність розробляти та управляти проектами.* *14.Здатність оцінювати та забезпечувати якість виконуваних робіт.* *15.Прагнення до збереження навколишнього середовища.*		ПК-8	**Виробнича компетентність** – здатність і готовність здійснювати ефективну професійну діяльність у відповідній галузі, надавати інфокомунікаційні послуги та послуги безпеки; здатність до планування й реалізації заходів із захисту інформації в ІКС, створення та забезпечення функціонування систем ІКБ; здатність до формування правильних висновків, оперативного приймання та реалізації нестандартних рішень тощо.

Безумовно, найменш зрозумілою й тому, імовірно, найбільш складною задачею в цьому процесі є розробка стандарту вищої освіти зі спеціальності 125 «кібербезпека» та освітньо-наукових програм, за тепер вже, спеціалізаціями «Безпека інформаційно-комунікаційних систем» (БІКС), «Системи технічного захисту інформації» (СТЗІ) та «Управління інформаційною безпекою» (УІБ) на бакалаврському освітньо-професійному рівні. Й тому є певні, зрозумілі всім пояснення. Так, наприклад:

завдання із забезпечення безпеки ІКС (технічний захист інформації (ТЗІ) від несанкціонованого доступута криптографічний захист інформації (КЗІ)), а також управління ІБ (відповідно до стандартів серії ISO/IEC 2700X) – є актуальними лише для фахівців із БІКС та УІБ;

завдання із захисту об'єктів інформаційної діяльності від витоку акустичної інформації, побічних електромагнітних випромінювань та наведень ІКТ, силових впливів на технічні засоби тощо – є зрозумілими лише для фахівців із ТЗІ й залишаються поза увагою фахівців інших спеціалізацій.

Тим не менш, в навчальних планах підготовки цих фахівців може бути виділена спільна частина навчальних дисциплін, по-перше, в циклах загальної та професійної підготовки, яка стосується, наприклад, основ ІКТ та ІКС, основ програмної і комп'ютерної інженерії, основ управління ІБ, методів, засобів та заходів ТЗІ і КЗІ й, по-друге, в циклі дисциплін вільного вибору студентів, які стосуються їх курсової підготовки, наприклад, викладання основ мережевої та CCNA безпеки, стандартів безпеки, прикладних аспектів сучасних технологій програмування в інформаційній та кібербезпеці тощо (табл.2).

Таблиця 2

Дисципліни спеціальності «кібербезпека», найбільш цікаві з точки зору майбутніх працедавців

Освітньо-професійний рівень	
бакалавр	магістр
Кібернетичний простір Основи інформаційної та кібербезпеки Безпека ІКС та протоколів обміну Безпека сховищ даних Прикладна криптологія Криптомеханізми інформаційної та кібербезпеки Інформаційно-аналітичне забез-печення систем ІБ, Інформаційна та кібербезпека сучасного підприємства	Технології виявлення злоякісного програмного забезпечення Технології виявлення уразливостей мережевих ресурсів Технології розробки програмного забезпечення систем інформаційної та кібербезпеки Безпека мережевої інфраструктури Технології виявлення уразливості Web-ресурсів Управління інцидентами інформаційної безпеки

Необхідна деталізація підготовки фахівців за кожною із спеціалізацій має бути передбачена у варіативних частинах їх освітньо-наукових програм. Варіант реалізації таких пропозицій для освітньо-професійного рівня «бакалавр» подано на рис.1.

Висновки

Зважаючи, що останнім часом ІКТ все частіше використовуються для

можливість застосування проти нашої держави низки кібератак і кібероперацій, які можуть призвести до проблем, пов'язаних із забезпеченням безперебійного функціонування об'єктів критичної інфраструктури, цілісності та конфіденційності інформації, а також її збереження, тобто всього того, з чим вже зіштовхнулась більшість країн Заходу – залишається актуальною.

З метою убезпечення від таких дій постає потреба у проведенні, перш за все, інформаційно-пропагандистської кампанії про значимість проблематики інформаційної та кібербезпеки, а також підвищенні компетентності фахівців різних сфер діяльності з цих питань. При цьому за доцільне вбачається *фахову підготовку фахівців з інформаційної і кібербезпеки* для потреб як силових структур та органів державного управління, так і виробничої та банківської сфери проводити у єдиній системі освіти України, а *спеціальну підготовку офіцерського складу ЗС України та інших силових структур* із загальних питань – в системі командирської підготовки та на курсах підвищення кваліфікації. Виходячи з досвіду іноземних країн та особливостей українських реалій, вирішення цих завдань неможливе без:

1) створення єдиного координуючого органу в сфері телекомунікацій та інформатизації, складовими сегментами якого мають бути:

Національний центр кіберзахисту та протидії кіберзагрозам з функціями виявлення та оцінки кібернетичних загроз національним інтересам і безпеці України, розробки концептуальних засад та надання рекомендацій державним і комерційним структурам з протидії зазначеним загрозам, здійснення активної протидії кібернетичним атакам противника та впливу на їх інформаційні системи;

органи власної інформаційної та кібербезпеки державних установ та комерційних організацій, які повинні взаємодіяти з Національним центром з питань вироблення єдиної політики щодо захисту як власного, так і спільного національного інформаційного та кібернетичного просторів;

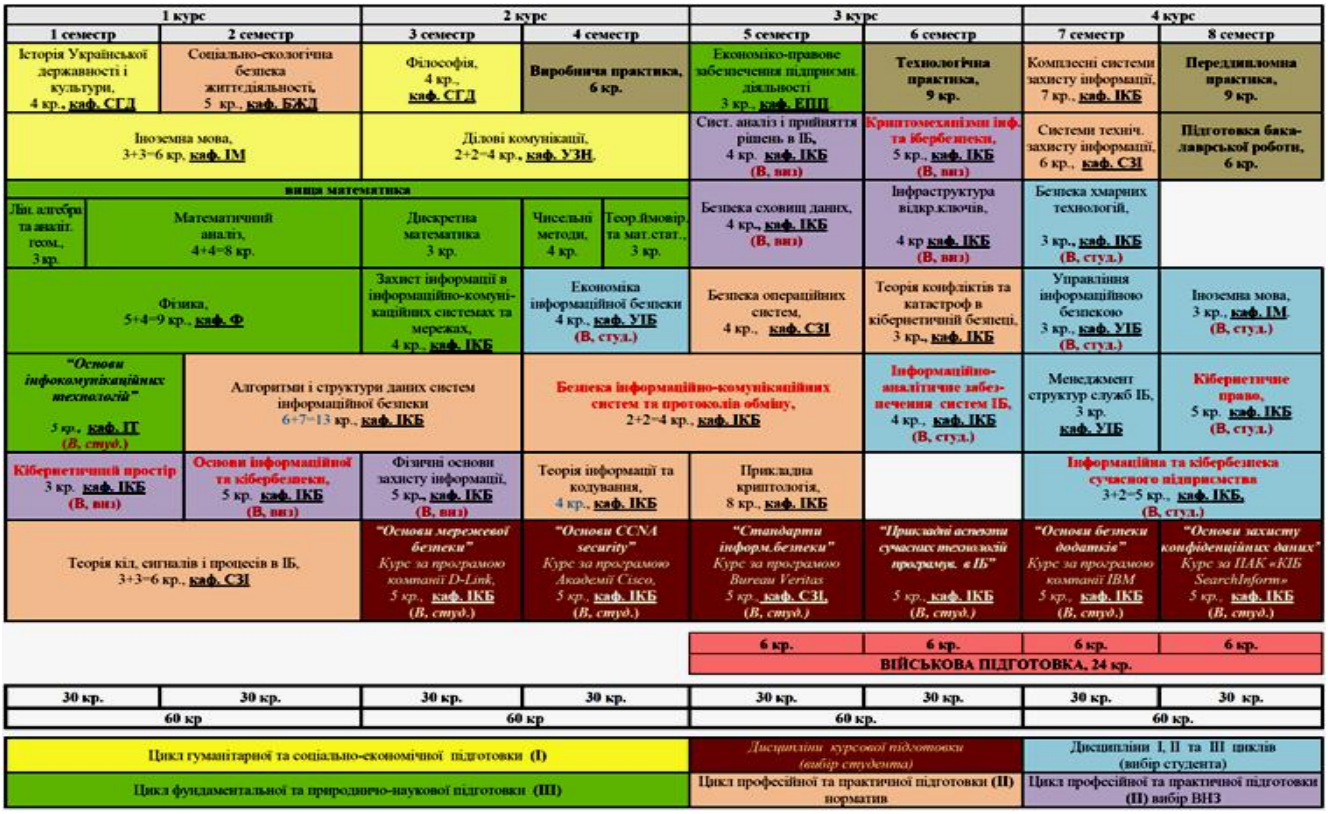

Рис.1. Структурно-логічна схема проходження дисциплін спеціалізації «безпека інформаційно-комунікаційних систем» освітньо-професійного рівня «бакалавр»

2) формування нормативної бази, яка б відповідала вимогам світових стандартів. Швидкого ефекту можна досягти, використовуючи документи, які вже перекладені на українську мову й готові до застосування – це, наприклад, стандарт забезпечення інформаційної безпеки ISO-27001/ISO-27002, переведений Національним Банком України та стандарт IT-управління Cobit, розроблений міжнародною асоціацією управління ISACA.

Такий підхід, як результат, дозволить:

охопити низку проблем сфери кібернетичної безпеки, пов'язаних із захистом інформації особи, суспільства та держави (включаючи завдання УІБ та ТЗІ);

визначити нормативний термін і зміст навчання та нормативні форми державної атестації, а також встановити вимоги до змісту, обсягу й рівня освіти та професійної підготовки такого випускника;

адаптувати зміст підготовки фахівців у ВНЗ до сучасних і перспективних потреб інформаційної та кібербезпеки;

забезпечити відповідний рівень взаємодії з ВНЗ провідних країн світу з питань вдосконалення підготовки фахівців у галузі інформаційної та кібербезпеки;

скоординувати дії силових (спеціалізованих) державних та бізнесових структур у підготовці компетентних і кваліфікованих фахівців з інформаційної та кібербезпеки тощо.

Література

1. Руководство по кибербезопасности для развивающихся стран. [Електронний ресурс]. – Режим доступу: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-r.pdf.

2. National Strategy to Secure Cyberspace. U.S. government via Department of Homeland Security. February 2003. p. 16. Retrieved 2008-05-18. [Електронний ресурс]. – Режим доступу: ttp://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

3. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.

4. «Про вищу освіту». Закон України від 1.07.2014 року № 1556-VII

5. «Про Стратегію кібербезпеки України». Указ Президента України №96/2016 від 27 січня 2016 року.

6. Buryachok V., Bogush V. Guidelines for the development and implementation training profile «cyber security» in Ukraine // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 126-131.

7. Сисоєв В. Аналіз рівня освіти та підготовки фахівців з управління ІТ та інформаційної безпеки в Україні. Режим доступу: http://www.auditagency.com.ua/blog/ISACA_research_ Education.pdf.

8. Даник Ю.Г., Супрунов Ю.М. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України. Збірник наукових праць ЖВІ НАУ «Інформаційні системи». Випуск 5. – 2011. – С.5- 22.

9. Міночкін А. І. Інформаційна боротьба: сучасний стан та досвід підготовки фахівців / А. І. Міночкін // Оборонний вісник. – К. : Центр воєнної політики та політики безпеки, 2011. – № 2. – С. 12–14.

Надійшла 15.04.2016 р. Рецензент: д.т.н., проф. Шевченко В.Л.