Міністерство освіти і науки України
Вінницький національний технічний університет

ЗАТВЕРДЖУЮ
Ректор Вінницького національного технічного університету
_____ В. В. Грабко
(підпис)
«_30_» ___08___ 2018 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ МАГІСТРІВ

за спеціальністю 125 – Кібербезпека
ІІ (магістерський) рівень вищої освіти

Назва освітньо-професійної програми
Безпека інформаційних і комунікаційних систем

(освітньо-професійна програма затверджена Вченою радою
Вінницького національного технічного університету
протокол № 1 від 30.08.2018 р.)

Галузь науки – 12 Інформаційні технології
Кваліфікація – Магістр з кібербезпеки

Термін навчання – 1 рік 4 місяців
Форма навчання – денна та заочна

Передмова

1. РОЗРОБЛЕНО у Вінницькому національному технічному університеті кафедрою захисту інформації (ЗІ)

2. ВНЕСЕНО Вінницьким національним технічним університетом

3. РОЗРОБНИКИ

1. Лужецький Володимир Андрійович, ВНТУ, д.т.н., професор, завідувач кафедри захисту інформації.
2. Войтович Олеся Петрівна, ВНТУ, к.т.н., доцент, доцент кафедри захисту інформації.

Зміст

Вступ

Освітня програма (далі – ОП) підготовки магістрів за спеціальністю 125 «Кібербезпека» розроблена з врахуванням пропозицій Науково-методичної ради Міністерства освіти і науки України, Науково-методичної підкомісії за спеціальністю 125 – «Кібербезпека», галузевих об’єднань роботодавців.

Освітня програма підготовки бакалавра за спеціальністю 125 «Кібербезпека» розроблена колективом професорсько-викладацького складу кафедри захисту інформації факультету інформаційних технологій та комп’ютерної інженерії Вінницького національного технічного університету.

1 Загальна характеристика

Рівень вищої освіти	Другий (магістерський) рівень
Освітній ступінь, що присвоюється	Магістр
Назва галузі знань	12 Інформаційні технології
Назва спеціальності	125 Кібербезпека
Обмеження щодо форм навчання	Денна, заочна
Кваліфікація освітня, що присвоюється	магістр з кібербезпеки
Кваліфікація в дипломі	Ступінь вищої освіти - Магістр Спеціальність - 125 Кібербезпека Освітньо-професійна програма - Безпека інформаційних і комунікаційних систем
Опис предметної області	Об’єкти професійної діяльності випускників: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту. Цілі навчання підготовка професіоналів, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Теоретичний зміст предметної діяльності Знання: – основні поняття і концепції в галузі кібербезпеки; – методи моніторингу та аудиту безпеки кіберпростору; – методи проектування систем та комплексів забезпечення інформаційної та кібербезпеки; – методи оцінювання та забезпечення відповідного рівня захищеності інформації; – методи та засоби ідентифікації вразливостей та загроз інформаційної та кібербезпеки; – методи аналізу та планування основних економічних показників проектних рішень. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. Інструменти та обладнання:

	– системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних систем.
Академічні права випускників	– продовження освіти за третім (освітньо-науковим) рівнем вищої освіти для отримання ступеня доктора філософії за спеціальністю 125 Кібербезпека або іншими спорідненими (суміжними) спеціальностями галузі знань 12 Інформаційні технології, що узгоджуються з отриманим дипломом магістра, іншими міждисциплінарними магістерськими програми

Працевлаштування випускників

КОД КП	КОД ЗКППТР	ВИПУСК ДКХП	Професійна назва роботи
2149.2			Професіонал із організації інформаційної безпеки
2149.2			Професіонал із організації захисту інформації з обмеженим доступом
International Standard Classification of Occupations 2008 (ISCO-08)			
Code			Occupation
2529			Specialist, security: data
2529			Specialist, security: ICT

2 Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти

Обсяг освітньо-професійної програми підготовки магістра становить 90 кредитів ЄКТС.

3 Перелік компетентностей випускника

Інтегральна компетентність

Здатність розв’язувати складні задачі і проблеми у галузі інформаційної та кібербезпеки або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.

Загальні компетентності

ЗК-1 Здатність застосовувати знання у практичних ситуаціях.
ЗК-2 Здатність спілкуватися іноземною мовою та вести професійну, у тому числі науково-дослідну діяльність, у міжнародному середовищі.

ЗК-3 Здатність здійснювати професійну діяльність згідно з вимогами санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки
ЗК-4 Навички виконання завдань науково-дослідної, науково-педагогічної, управлінської і інноваційної діяльності;
ЗК-5 Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК-6 Здатність аналізувати, верифікувати, оцінювати повноту інформації в ході професійної діяльності, за необхідності доповнювати й синтезувати відсутню інформацію й працювати в умовах невизначеності.
ЗК-7 Здатність приймати обґрунтовані рішення.
ЗК-8 Здатність проводити розрахунки з техніко-економічного обґрунтування та функціонально-вартісного аналізу ефективності проектних рішень, включаючи оцінку інноваційних ризиків комерціалізації проектів.

Спеціальні (фахові, предметні) компетентності

СП-1 Здатність застосовувати системний підхід до вирішення проблем інформаційної та кібербезпеки;
СП-2 Здатність застосовувати відповідні математичні, наукові і технічні методи, а також спеціалізоване програмне забезпечення для вирішення завдань в сфері інформаційної та кібербезпеки;
СП-3 Здатність використовувати практичні навички в сфері інформаційної та кібербезпеки;
СП-4 Здатність продемонструвати знання і розуміння наукових фактів, концепцій, теорій, принципів і методів, необхідних для підтримки спеціалізацій з інформаційної та кібербезпеки;
СП-5 Здатність продемонструвати розуміння проблем інформаційної та кібербезпеки;
СП-6 Здатність продемонструвати розуміння питань використання технічної літератури та інших джерел інформації
СП-7 Здатність виявляти і описувати ефективність рішень в сфері інформаційної та кібербезпеки на основі використання аналітичних методів і методів моделювання;
СП-8 Здатність продемонструвати знання і розуміння математичних принципів і методів, необхідних для підтримки спеціалізацій з інформаційної та кібербезпеки;
СП-9 Здатність розробляти плани і проекти для забезпечення досягнення поставленої певної мети з урахуванням всіх аспектів вирішуваної проблеми
СП-10 Здатність продемонструвати розуміння вимог до діяльності в сфері інформаційної та кібербезпеки.

4 Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання

Результати навчання за загальними компетентностями:

1. Знання і розуміння основних понять інформаційної та кібербезпеки, а також сучасних викликів у забезпеченні безпеки кіберпростору відповідно до найновіших досліджень, на рівні необхідному для досягнення інших результатів програми, в тому числі певна обізнаність в останніх досягненнях.
2. Уміння представляти та обговорювати наукові результати іноземною мовою (англійською або іншою, відповідно до специфіки спеціальності) в усній та письмовій формах, приймати участь у наукових дискусіях і конференціях.
3. Уміти створювати та забезпечувати безпечні умови діяльності, у тому числі в надзвичайних ситуаціях.
4. Спроможність аналізувати складні інженерні задачі, процеси і системи відповідно до спеціалізації; обирати і застосовувати придатні типові аналітичні, розрахункові та експериментальні методи; уміння інтерпретувати результати таких досліджень.
5. Уміти планувати та здійснювати власне наукове дослідження, присвячене суттєвій проблемі сучасної науки у галузі інформаційної та кібербезпеки.
6. Уміти викладати у вищому навчальному закладі предметів, що стосуються галузі кібербезпеки, а також розробляти методичні матеріали, що використовуються студентами в навчальному процесі.
7. Використовуючи знання форм і методів наукового пізнання застосовувати їх у галузі інформаційних технологій та кібербезпеки.
8. Здатність використовувати методи загальнонаукового аналізу у галузі кібербезпеки та показувати можливості сучасних природничо-наукових методів дослідження у практиці забезпечення інформаційної та кібербезпеки
9. Здатність проводити бібліографічну роботу із залученням сучасних інформаційних технологій, формувати цілі дослідження, складати техніко-економічне обґрунтування досліджень, що проводяться, вибирати необхідні методи дослідження, модифікувати існуючі та розробляти нові методи, виходячи із завдань конкретного дослідження, застосовувати сучасні методи проведення експерименту в конкретній галузі знань
10. Уміти проводити розрахунки з техніко-економічного обґрунтування та функціонально-вартісного аналізу ефективності проектних рішень, включаючи оцінку інноваційних ризиків комерціалізації проектів.

Результати навчання за спеціальними (фахові, предметні) компетентностями:

Компетентності, якими повинен оволодіти здобувач	Програмні результати навчання	Найменування навчальних дисциплін, практик
1. Здатність застосовувати системний аналіз прикладної області, виявлення загроз і оцінка вразливості інформаційних систем, розробка вимог і критеріїв інформаційної безпеки, узгоджених зі стратегією розвитку інформаційних систем	**Вміти:** - розробляти математичні моделі завдань забезпечення інформаційної безпеки та захисту інформації - використовувати математичні методи оптимізації з метою одержання найкращих характеристики функціонування засобів та систем;	**2.1.1.1** Математичні методи моделювання та оптимізації процесів
	Знати: - сучасні методи та основи аналізу прикладної області; - основи моделювання. загроз, вразливостей, ризиків інформаційної та кібербезпеки	
	Вміти: - використовувати сучасне програмне забезпечення, методики проектування, аналізу та моделювання інформаційних систем; - вирішувати задачу обробки статистичних даних за допомогою ЕОМ, моделювати за допомогою ЕОМ	1.2.4. Сучасні інформаційні технології в кібербезпеці
	Знати: - сучасні методи проектування, аналізу та моделювання інформаційних систем; - основи комп'ютерного моделювання складних систем.	
	Вміти: - самостійно аналізувати та визначати зовнішні та внутрішні загрози в кіберпросторі; - використовувати засоби для моніторингу та аудиту кіберпростору.	2.2.1.1.1 Моніторинг та аудит кіберпростору
	Знати: - основні загрози, вразливості та ризики відповідно до розвитку інформаційних систем; - основи аудиту інформаційної безпеки, визначення захищеності інформаційно-комунікаційної системи;	
	Вміти: - розробляти вимоги і критеріїв інформаційної та кібербезпеки безпеки відповідно до сучасного розвитку кіберпростору; - синтезувати правила політики інформаційної безпеки відповідно до стратегії розвитку інформаційних систем та нормативно-правової бази.	**2.2.1.2.2** Методи аналізу та синтезу політик інформаційної безпеки
	Знати: - загальні технічні вимоги до забезпечення необхідного рівня захищеності інформаційних ресурсів; - методи аналізу та синтезу політки інформаційної безпеки відповідно до стратегії розвитку інформаційних систем та нормативно-правової бази.	
2. Здатність застосовувати відповідні	**Вміти:** - будувати інформаційну модель; - застосовувати інформаційні технології та обчислювальні експерименти;	1.2.4. Сучасні інформаційні технології в кібербезпеці

математичні, наукові і технічні методи, а також спеціалізоване програмне забезпечення для вирішення завдань в сфері інформаційної та кібербезпеки;	- визначати модель актуальних загроз та оцінювання ризиків.	
	Знати: - методи моделювання сучасних інформаційних систем та систем кібербезпеки; - інформаційні технології кібербезпеки на основі систем підтримки прийняття рішень; - Показники оцінювання рівня кібербезпеки	
	Вміти: - оцінювати поточний стан рівня інформаційної та кібербезпеки; - аргументувати вибір та застосовування методів і засобів для побудови захищених інформаційних систем у кіберпросторі	1.2.3 Кібербезпека
	Знати: - методи та засоби проведення досліджень з кібербезпеки, спираючись на сучасні досягнення світової науки і передові технології.	
	Вміти: - розробляти математичні моделі систем і процесів, які максимально адекватно відображають їх роботу або функціонування в реальних умовах експлуатації; - самостійно моделювати технологічні процеси об'єктів з метою отримання найефективніших результатів	2.1.1.1 Математичні методи моделювання та оптимізації процесів
	Знати: - основні питання теоретичних підходів щодо методів моделювання систем і процесів; - методи аналізу математичних моделей аналітичними і чисельними способами.	
	Вміти: - використовувати існуючі пакети програм для створення і експлуатації систем, створених на основі інтернет-технологій; - застосовувати методи та прийоми проектування захищених інформаційних та комунікаційних систем. - оцінювати відповідність системи захисту стандартам інформаційної безпеки;	2.1.1.2 Технології створення та застосування систем захисту в кіберпросторі
	Знати: - загальна технологія розробки комплексів засобів захисту інформаційно-комунікаційних систем. - основи проектування системи захисту. - типові методи та прийоми проектування захищених інформаційних та комунікаційних систем. - принципи оптимізації процесів проектування захищених інформаційних та комунікаційних систем	
	Вміти: - використовувати методи аналізу та синтезу криптосистем; - застосовувати методи та прийоми проектування криптографічних протоколів. - оцінювати відповідність системи захисту стандартам інформаційної безпеки;	2.1.1.3 Методи побудови та аналізу криптосистем

	Знати: - технологію розробки криптографічних систем, включно з алгоритмами шифрування, гешування, автентифікації тощо; - типові методи та прийоми проектування криптографічних методів та протоколів; - принципи та методи криптоаналізу.	
3. Здатність використовувати практичні навички в сфері інформаційної та кібербезпеки	**Вміти:** - оцінювати поточний стан рівня безпеки; - аргументувати вибір та застосовування методів і засобів для побудови захищених інформаційних систем у кіберпросторі; - розробляти рекомендації щодо удосконалення системи інформаційної безпеки.	**1.2.5** Кібербезпека
	Знати: - сучасну нормативну базу у галузі інформаційної та кібербезпеки; - методи та засоби забезпечення кібербезпеки програмних застосунків, віддалених інформаційних серверів, кінцевих користувачів; - методи та засоби підтримки готовності систем, та захисту від методів соціальної інженерії; - особливості побудови критичних систем та вимоги забезпечення їх кібербезпеки .	
	Вміти: - використовувати та засоби для моніторингу та аудиту кіберпростору; - обґрунтовувати застосування методів та засобів забезпечення кібербезпеки;.	**2.2.1.1.1** Моніторинг та аудит кіберпростору
	Знати: - стандартизацію у галузі моніторингу систем інформаційної та кібербезпеки; - основи аудиту інформаційної та кібербезпеки; - визначення захищеності системи; - аналіз ризиків і управління ризиками; - визначення ступеню відповідності інформаційної безпеки основним нормам і стандартам.	
	Вміти: - розробляти технічне завдання на проект системи захисту; - описувати технічні вимоги системи захисту; - реалізувати систему захисту інформації.	**2.1.1.2** Технології створення та застосування систем захисту в кіберпросторі
	Знати: - роботи із створення, виготовлення, монтажу, налагодження, випробування і здавання в експлуатацію систем і засобів забезпечення інформаційної безпеки; - керівні документи із створення, виготовлення, монтажу, налагодження, випробування і здавання в експлуатацію систем і засобів забезпечення інформаційної безпеки; - керівні документи щодо забезпечення робіт з удосконалення, модернізації, уніфікації систем, засобів і технологій забезпечення інформаційної безпеки.	
	Вміти: - виконувати розробку систем криптографічного захисту інформації; - аналізувати системи криптографічного захисту на стійкість, ресурсоємність, швидкодію тощо; - виконувати криптоаналіз методів криптографічного захисту інформації	**2.1.1.3** Методи побудови та аналізу криптосистем
	Знати:	

	- методи та засоби побудови криптосистем; - методи та засоби аналізу криптосистем.	
4. Здатність продемонструвати знання і розуміння наукових фактів, концепцій, теорій, принципів і методів, необхідних для підтримки спеціалізацій з інформаційної та кібербезпеки	**Вміти:** - самостійно аналізувати та визначати зовнішні та внутрішні загрози в кіберпросторі; - використовувати та налагоджувати різноманітні засоби для моніторингу та аудиту кіберпростору;	**2.2.1.1.1** Моніторинг та аудит кіберпростору
	Знати: - основні загрози та ризики кіберпростору; - основи функціонування систем моніторингу.	
	Вміти: - досліджувати інформаційні ресурси як інформаційних систем так і систем захисту інформації; - досліджувати продуктивність як інформаційних систем так і систем захисту інформації; - розробляти рекомендації стосовно організації та захисту розподілених інформаційних ресурсів.	**2.2.1.1.2** Організація та захист розподілених інформаційних ресурсів
	Знати: - нормативно-правову документацію стосовно захисту розподілених інформаційних ресурсів; - теорію продуктивності інформаційних систем; - принципи, методи та засоби захисту розподілених інформаційних ресурсів на всіх етапах життєвого циклу.	
	Вміти: - збирати і проводити аналіз інформації, що циркулює у критичних системах; - виконувати аналіз загроз та вразливостей (внутрішніх та зовнішніх) критичних систем; - оцінювати ризики інформаційних ресурсів критичних систем; - визначати рекомендації щодо забезпечення кібербезпеки критичних систем; - проектувати та будувати системи забезпечення безпеки критичних систем.	**2.2.1.2.1** Кібербезпека критичних систем
	Знати: - принципи функціонування критичних систем; - сучасні атаки на критичні системи; - методи та засоби оцінювання ризиків; - принципи, методи та засоби виявлення вразливостей критичних систем; - принципи, теорії, методи проектування та побудови критичних систем; - принципи, теорії, методи проектування та побудови систем забезпечення кібербезпеки критичних систем.	
	Вміти: - аналізувати відомі політики безпеки; - пропонувати правила та розділи політики безпеки відповідно до сучасних викликів інформаційної та кібербезпеки; - оцінювати ризики інформаційних ресурсів; - розробляти сучасні політики інформаційної безпеки;	2.2.1.2.2 Методи аналізу та синтезу політик інформаційної безпеки
	Знати: - нормативно-правові акти, як українські та к і міжнародні у галузі кібербезпеки, зокрема побудови політик інформаційної безпеки;	

	- концепцій, теорій, принципів і методів, необхідних для розробки політик інформаційної безпеки; - принципи, теорії, методи проектування та побудови систем підтримки прийняття рішень щодо побудови політик інформаційної безпеки..	
5. Здатність продемонструвати розуміння проблем інформаційної та кібербезпеки	**Вміти:** - визначати нові вразливості та атаки нульового дня в інформаційних ресурсах та системах; - проектувати та розробляти системи забезпечення кібербезпеки відповідно до нових атак та вразливостей .	**1.2.5** Кібербезпека
	Знати: - методи та засоби виявлення та аналізу вразливостей та атак на кіберпростір. - офіційні та неофіційні ресурси, на яких публікуються виявлені вразливості та атаки	
	Вміти: - розробляти та документально супроводжувати процес проектування систем забезпечення кібербезпеки; - оцінювати ефективність відомих та розроблених методів та засобів забезпечення інформаційної та кібербезпеки.	**2.1.1.2** Технології створення та застосування систем захисту в кіберпросторі
	Знати: - методи та принципи проектування засобів захисту в кіберпросторі; - нормативну документацію з розробки та забезпечення інформаційної та кібербезпеки.	
6. Здатність продемонструвати розуміння питань використання технічної літератури та інших джерел інформації	**Вміти:** - проводити інформаційний пошук у технічній літературі та різноманітних джерелах, в тому числі Інтернет-базах наукової та дослідницької літератури; - виокремлювати потрібну і достовірну інформацію з різних джерел на основі аналізу.; - проводити аналіз результатів, отриманих іншими науковцями.	**1.2.3** Методологія та організація наукових досліджень в кібербезпеці
	Знати: - методи та принципи інформаційного пошуку у сучасних базах наукової та дослідницької літератури; - питання використання різноманітної літератури; - принципи визначення плагіату.	
7. Здатність виявляти і описувати ефективність рішень в сфері інформаційної та кібербезпеки на основі використання аналітичних методів і методів моделювання	**Вміти** - планувати, проводити та оцінювати результати науково-дослідної роботи, - обґрунтовувати доцільність розробки та впровадження; - застосовувати кількісні та якісні методи при аналізі ефективності розробки; - розробляти інформаційні проекти та проводити їх оцінку.	**1.2.4** Економічне обґрунтування інноваційних рішень в галузі інформаційних технологій
	Знати: - принципи та методи оцінювання ефективності науково-дослідних робіт; - сутність і зміст методів планування науково-дослідних та дослідно-конструкторських робіт; - методи та засоби розробки інформаційних проектів та проведення їх оцінювання	

	Вміти: - розробляти математичні моделі систем і процесів у галузі інформаційної та кібербезпеки; - застосовувати методи аналізу отриманих моделей з метою отримання тих параметрів, які забезпечують функціонування їх реальних прототипів у найефективніший спосіб; - самостійно моделювати рішення у галузі інформаційної та кібербезпеки.	2.1.1.1 Математичні методи моделювання та оптимізації процесів
	Знати: - основні питання теоретичних підходів щодо методів моделювання систем і процесів; - методи підтримки прийняття рішень в задачах інформаційної та кібербезпеки.	
8. Здатність продемонструвати знання і розуміння математичних принципів і методів, необхідних для підтримки спеціалізацій з інформаційної та кібербезпеки	**Вміти:** - моделювати зовнішні та внутрішні загрози в кіберпросторі; - розробляти системи підтримки прийняття рішення в системах аудиту інформаційної та кібербезпеки;	**2.2.1.1.1** Моніторинг та аудит кіберпростору
	Знати: - Принципи та способи моделювання загроз, вразливостей та оцінювання ризиків; - Методи прийняття рішення в системах аудиту інформаційної та кібербезпеки.	
	Вміти: - досліджувати інформаційні ресурси як інформаційних систем так і систем захисту інформації; - проектувати та розробляти системи оцінювання продуктивності як інформаційних систем так і систем захисту інформації.	**2.2.1.1.2** Організація та захист розподілених інформаційних ресурсів
	Знати: - теорію продуктивності інформаційних систем; - принципи, методи та засоби розробки систем захисту розподілених інформаційних ресурсів на всіх етапах життєвого циклу.	
	Вміти: - збирати і проводити аналіз інформації, що циркулює у критичних системах; - оцінювати ризики інформаційних ресурсів критичних систем; - проектувати та будувати системи забезпечення безпеки критичних систем.	**2.2.1.2.1** Кібербезпека критичних систем
	Знати: - методи та засоби оцінювання ризиків; - принципи, теорії, методи проектування та побудови систем забезпечення кібербезпеки критичних систем.	
	Вміти: - оцінювати ризики інформаційних ресурсів; - розробляти системи підтримки прийняття рішень для формування політики інформаційної безпеки;	2.2.1.2.2 Методи аналізу та синтезу політик інформаційної безпеки
	Знати: - принципи, теорії, методи проектування та побудови систем підтримки прийняття рішень щодо побудови політик інформаційної безпеки..	
9. Здатність	**Вміти:**	**2.1.1.2** Технології

розробляти плани і проекти для забезпечення досягнення поставленої певної мети з урахуванням всіх аспектів вирішуваної проблеми	- застосовувати методи та прийоми проектування захищених інформаційних та комунікаційних систем; - розробляти технічне завдання на систему захисту; - описувати технічні вимоги системи захисту; - реалізувати систему захисту інформації; - розробляти робочу документацію на систему захисту;. - розробляти методику випробовувань системи захисту; - розробляти керівні документи щодо створення, виготовлення, монтажу, налагодження, випробування і здавання в експлуатацію систем і засобів забезпечення інформаційної безпеки.	створення та застосування систем захисту в кіберпросторі
	Знати: - етапи розробки проекту комплексу засобів захисту інформаційно-комунікаційної системи. - принципи розробки проектної документації. - принципи розробки та методики випробувань.	
10. Здатність продемонструвати розуміння вимог до діяльності в сфері інформаційної та кібербезпеки	**Вміти:** - використовувати експериментальний підхід до реалізації та компонування криптографічних систем; - пропонувати обґрунтований вибір та застосовування засобів, необхідних для реалізації та компонування криптографічних систем - оцінювати показники запропонованих криптосистем;	2.1.1.3 Методи побудови та аналізу криптосистем
	Знати: - методи, засоби та методики оцінювання крипто протоколів за стійкістю, ресурсоємністю, швидкодією тощо; - сучасні вимоги, яких необхідно досягати при побудови криптосистем;	
	Вміти: - описувати технічні вимоги системи захисту; - оцінювати відповідність системи захисту стандартам інформаційної безпеки.	**2.1.1.2** Технології створення та застосування систем захисту в кіберпросторі
	Знати: - керівні документи із створення, виготовлення, монтажу, налагодження, випробування і здавання в експлуатацію систем і засобів забезпечення інформаційної безпеки. - керівні документи щодо забезпечення робіт з удосконалення, модернізації, уніфікації систем, засобів і технологій забезпечення інформаційної безпеки	

5 Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти

Атестація здійснюється атестаційною комісією після виконання студентом навчального плану та завершується видачою диплома встановленого зразка.

На атестацію виноситься нормативний і варіативний зміст підготовки фахівця.

Термін проведення атестації визначається навчальним планом та графіком освітнього процесу.

До атестації допускаються студенти, які виконали всі вимоги освітньо-наукової програми та навчального плану.

Результати атестації визначаються оцінками за національною шкалою «відмінно», «добре», «задовільно», «незадовільно».

Форма випускної атестації – атестація здійснюється у формі публічного захисту кваліфікаційної роботи на відкритому засіданні екзаменаційної комісії.

Вимоги до випускної кваліфікаційної роботи

Кваліфікаційна робота має передбачати дослідження та розв'язання спеціалізованого завдання або практичної проблеми в предметній області діяльності випускника, що характеризується комплексністю та невизначеністю умов.

В змісті кваліфікаційної роботи кожного випускника глибоко і обґрунтовано розкриваються розроблені їм питання з нормативного і варіативного змісту підготовки фахівця.

Кваліфікаційна робота має бути перевірена на плагіат.

Кваліфікаційна робота має бути розміщена в електронній базі ВНТУ

Вимоги до кваліфікаційного екзамену

Кваліфікаційний екзамен має передбачати оцінювання сукупності знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за даним стандартом.

6 Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

У ВНЗ функціонує система забезпечення якості освітньої діяльності (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду освітніх програм;

3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників вищого навчального закладу та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті вищого навчального закладу, на інформаційних стендах та в будь-який інший спосіб;

4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;

8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників вищих навчальних закладів і здобувачів вищої освіти;

9) інших процедур і заходів.

7 Перелік нормативних документів

1. Закон України «Про вищу освіту».

2. Постанова Кабінету Міністрів України від 23.11.2011 р. № 1341 «Про затвердження національної рамки кваліфікацій».

3. Постанова Кабінету Міністрів України від 29.04.15 року № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти».

4. Класифікація видів економічної діяльності : ДК 009:2010. – На заміну ДК 009:2005 ; Чинний від 2012-01-01. – (Національний класифікатор України).

5. Класифікатор професій ДК 003:2010. – На заміну ДК 003:2005; Чинний від 2010-11-01. – (Національний класифікатор України).

6. Области образования и профессиональной подготовки 2013 (МСКО-О 2013): Сопроводительное руководство к Международной стандартной классификации образования 2011. – Институт статистики ЮНЕСКО, 2014. – Режим доступу : http://www.uis.unesco.org/Library/Documents/isced-f-2013-fields-of-education-training-2014-rus.pdf.

7. Національний освітній глосарій: вища освіта / 2-е вид., перероб. і доп. / авт.-уклад. : В. М. Захарченко та ін. / За ред. В. Г. Кременя. – К. : ТОВ «Видавничий дім «Плеяди», 2014. – 100 с.

8. Розроблення освітніх програм. Методичні рекомендації / Авт.: В.М. Захарченко, В.І. Луговий, Ю.М. Рашкевич, Ж.В. Таланова / За ред. В.Г. Кременя. – К.: ДП «НВЦ «Пріоритети», 2014. – 120 с.

9. Методичні рекомендації щодо розроблення стандартів вищої освіти / Схвалено сектором вищої освіти Науково-методичної Ради Міністерства освіти і науки України протокол № 3 від 29.03.2016.

10. Наказ Міністерства освіти і науки України 25.07.2013 р. № 1039 Про затвердження і введення в дію складових галузевих стандартів вищої освіти із спеціальностей освітньо-кваліфікаційного рівня «магістр» галузі знань 1701 «Інформаційна безпека» (за спеціальностями: 8.17010101 «Безпека інформаційних і комунікаційних систем»; 8.17010102 «Безпека державних інформаційних ресурсів»; 8.17010201 «Системи технічного захисту інформації, автоматизація її обробки»).