МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чернігівський національний технологічний університет
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

КІБЕРБЕЗПЕКА

Другого (магістерського) рівня вищої освіти

за спеціальністю 125 «Кібербезпека»

галузь знань 12 Інформаційні технології

Кваліфікація: магістр з кібербезпеки

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради

_____ /С.М. Шкарлет/

(протокол № 7 від «27» серпня 2019 р.)

Освітня програма вводиться в дію з 01 вересня 2019 р.

Ректор_____ / С.М. Шкарлет /

(наказ № 94 від «27» серпня 2019 р.)

Чернігів 2019 р.

ПЕРЕДМОВА

Розроблено проектною робочою групою (науково-методичною комісією спеціальності № 125 «Кібербезпека») у складі:

1. Ю.М. Ткач, д.пед.н., доцент, завідувач, професор кафедри кібербезпеки та математичного моделювання (керівник проектної групи).
2. М.Є. Шелест, д.т.н., проф., професор кафедри кібербезпеки та математичного моделювання.
3. В.І. Гур'єв, к.т.н., доцент, професор кафедри кібербезпеки та математичного моделювання.

Розроблено як тимчасовий документ до затвердження відповідного стандарту вищої освіти України за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для другого (магістерського) рівня вищої освіти.

1. Профіль освітньої програми зі спеціальності 125 «Кібербезпека»

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Чернігівський національний технологічний університет. ННІ Технологій. Факультет електронних та інформаційних технологій. Кафедра кібербезпеки та математичного моделювання
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр. Магістр з кібербезпеки
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Тип диплому – одиничний. Диплом магістра, одиничний, 90 кредитів ЄКТС., Термін навчання 1 рік 4 місяці
Наявність акредитації	Ліцензія: наказ МОН від 06.03.2019 року № 175-л Первинна акредитація
Цикл/рівень	НРК України - 8 рівень, QF-EHEA – другий цикл, EQF-LLL - 7 рівень
Передумови	Наявність ступеня бакалавра
Мова (и) викладання	Українська
Термін дії освітньої програми	До заміни новою
Інтернет адреса постійного розміщення опису освітньої програми	https://www.stu.cn.ua/staticpages/perelikrivniv/
2 – Мета освітньої програми	
Забезпечити студентам фундаментальну підготовку у вигляді поглиблених теоретичних і практичних знань, умінь та навичок за спеціальністю 125 Кібербезпека, достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузях телекомунікацій та інформаційних технологій, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу.	
3 – Характеристика освітньої програми	
Предметна область (галузь	Галузь знань – 12 «Інформаційні технології». Спеціальність – 125 «Кібербезпека»

знань, спеціальність, спеціалізація (за наявності))	
Орієнтація освітньої програми	Освітньо-професійна програма
Основний фокус освітньої програми та спеціалізації	Загальна: акцент на здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації.
Особливості програми:	Інтегрована підготовка фахівців до вирішення завдань у сфері інформаційної безпеки, що передбачає розроблення, впровадження та експлуатацію комплексних (інформаційних, телекомунікаційних, технічних) систем захисту інформації на об'єктах інформаційної діяльності, поглиблене вивчення нормативних документів та стандартів з захисту інформації, принципів побудови систем технічного захисту інформації, дій для захисту інформаційних ресурсів організацій і користувачів.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть працювати в державному та приватному секторах у таких сферах діяльності: 1)адміністрування ОС сімейства Windows/Linux, мережевого обладнання і технологій TCP/IP, DNS, DHCP, SSL/TLS, etc.; 2) застосування засобів антивірусного захисту (ESET, McAfee, Zilly, etc.), програмних, клієнт-серверних та хмарних технологій захисту інформації (систем веб фільтрації, систем запобігання вторгнень, систем захисту пошти від вірусів і спаму, etc.); 3)створення технічної, проектної та експлуатаційної документації інформаційно-комунікаційних систем (далі – ІКС)та систем захисту інформації (далі –СЗІ); 4)налагодження, експлуатації та проведення аналізу системних процесів функціонування мережевих, клієнт-серверних та хмарних технологій; 5)проведення моніторингу несанкціонованої активності в обчислювальних системах; 6)створення, впровадження та експлуатації комплексних систем захисту інформації (далі – КСЗІ), а також СЗІ в складі інформаційно-телекомунікаційних (далі – ІТС) та обчислювальних систем;

	7)формування політик та процесів у сфері ІТ безпеки, управління доступом до мережевих ресурсів ІТС та ризиками інформаційної безпеки; 8)проведення розслідувань інцидентів та забезпечення аудиту процесів інформаційної безпеки; 9)підтримка наукових досліджень, педагогічна діяльність тощо. Згідно з Національним класифікатором професій ДК 003:2010 фахівці, які здобули освіту за освітньою програмою «Кібербезпека» можуть обіймати такі посади, як: - програміст/тестувальник програмного забезпечення систем інформаційної та кібербезпеки; - адміністратор комп'ютерних систем і мереж; - адміністратор інформаційної та кібербезпеки; - аудитор/пентестер безпеки інформаційно-комунікаційних систем; - розробник засобів захисту інформації; - менеджер (управитель) систем з інформаційної безпеки; - професіонал із організації інформаційної безпеки; - професіонал із організації захисту інформації з обмеженим доступом.
Подальше навчання	Можливість здобуття освіти на третьому (освітньо-науковому) рівні вищої освіти за спеціальністю 125 «Кібербезпека» або іншими спорідненими (суміжними) спеціальностями галузі знань «Інформаційні технології», що узгоджуються з отриманим дипломом магістра, іншими міждисциплінарними магістерськими програми з ІТ компонентою. Можливість підвищення кваліфікації та отримання додаткової післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Ґрунтується на принципах студентоцентризму та індивідуально-особистісного підходу. Реалізується через навчання на основі досліджень, посилення практичної орієнтованості. Викладання проводиться у формі комбінації лекцій, мультимедійної лекції, інтерактивної лекції, практичних, лабораторних, самостійної навчальної та дослідницької роботи з використанням електронного навчання в системі Moodle, розв'язування прикладних задач, виконання курсового проекту (роботи), практики, кваліфікаційної магістерської роботи.
Оцінювання	Оцінювання навчальних досягнень здійснюється за 100-бальною (рейтинговою) шкалою ЕКТС (ECTS), національною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно»). Накопичувальна рейтингова система, що передбачає

	оцінювання студентів за всіма видами аудиторної та поза аудиторної освітньої діяльності, у вигляді поточного та семестрового контролю, а також атестації.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
	КЗ 2. Знання та розуміння предметної області та розуміння професії.
	КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово
	КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням
	КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
	КЗ 6. Здатність до відповідальності та навичок до безпечної діяльності відповідно до майбутнього профілю роботи, галузевих норм і правил, а також необхідного рівня індивідуального та колективного рівня безпеки у надзвичайних ситуаціях.
Фахові компетентності	КФ 1. Здатність розробляти та впроваджувати законодавчу, нормативно-правову базу, державні і міжнародні вимоги, а також інтегрувати, аналізувати і використовувати сучасні світові практики та стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
	КФ 2. Здатність розробляти, впроваджувати і супроводжувати програмні, програмно-апаратні та технічні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах (автоматизованих систем та їх додатків) та у інфраструктурі організації в цілому.
	КФ 3. Здатність виконувати моніторинг комп'ютерних мереж з метою виявлення зловживань та аномалій.
	КФ 4. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.
	КФ 5. Здатність розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, згідно встановленої політики інформаційної безпеки та/або кібербезпеки.

	КФ 6. Здатність формувати комплекс заходів для управління інформаційною безпекою, здійснювати управління інцидентами кібербезпеки, здійснювати управління ризиками інформаційної та кібербезпеки.
	КФ 7. Здатність розробляти, планувати, аналізувати та виконувати аудит та моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем.
	КФ 8. Здатність проводити науково-освітню діяльність, розробляти та впроваджувати систему управління персоналом.

ПРН	7 – Програмні результати навчання (ПРН)
1.	Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
2.	організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
3.	використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
4.	аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності,які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
5.	критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
6.	діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, в тому числі міжнародних в галузі інформаційної та/або кібербезпеки;
7.	впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
8.	забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
9.	використовувати програмні, програмно-апаратні та технічні комплекси захисту інформаційних ресурсів;
10.	вирішувати задачі управління процесами відновлення штатного функціонування ІТС з використанням процедур резервування згідно встановленої політики безпеки;

11.	вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
12.	розробляти та впроваджувати, супроводжувати системи аудиту та моніторингу якості бізнес процесів системи управління інформаційною безпекою та/або кібербезпекою;
13.	забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в ІТС;
14.	проводити та планувати навчання персоналу компанії, у відповідності до сучасних норм та вимог.

8 – Ресурсне забезпечення реалізації програм	
Кадрове забезпечення	Підготовку фахівців спеціальності 125 «Кібербезпека» забезпечують висококваліфіковані науково-педагогічні кадри університету включно з випусковою кафедрою.
Матеріально-технічне забезпечення	Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає потребі. В університеті діють власні об'єкти соціально-побутової інфраструктури. У тому числі: їдальня, буфети, гуртожитки, актові зали, спортивні зали, спортивні майданчики. Заняття та наукові дослідження проводяться у лабораторіях кафедри кібербезпеки, кафедри інформаційних і комп'ютерних систем, програмної інженерії та інформаційних технологій. Для проведення інформаційного пошуку та обробки результатів є комп'ютерні класи, де наявне відповідне програмне забезпечення та відкритий доступ до Інтернет-мережі.
Інформаційне та навчально-методичне забезпечення	Наукова бібліотека щороку поповнюється спеціалізованою літературою і періодичними виданнями, що відповідають напрямкам роботи кафедри. Використовуються технології електронного (дистанційного) навчання MOODLE.
9 – Академічна мобільність	
Національна кредитна мобільність	Індивідуальна академічна мобільність реалізується у рамках міжуніверситетських договорів про встановлення науково-освітянських відносин для задоволення потреб розвитку освіти і науки з університетами України. Допускається перезарахування кредитів, отриманих у інших університетах України, за умови відповідності їх набутих компетентностей.
Міжнародна кредитна мобільність	Академічна мобільність студентів здійснюється на підставі угод про співробітництво між іноземними закладами вищої

	освіти та ЧНТУ за узгодженими та затвердженими в установленому порядку індивідуальними навчальними планами та робочими програмами навчальних дисциплін. Студенти також реалізують своє право на міжнародну кредитну мобільність в рамках програми "Erasmus+".
Навчання іноземних здобувачів вищої освіти	-

2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти(роботи), практики, кваліфікаційна робота	Кількість кредитів	Форма підсумк. контролю
	2	3	4
Обов'язкові компоненти ОП			
ОК 1.	Цивільний захист та охорона праці в галузі	3	залік
ОК 2.	Іноземна мова (за професійним спрямуванням)	4	залік
ОК 3.	Методи побудови та аналізу криптосистем	5	залік
ОК 4.	Методологія та організація наукових досліджень	4	екзамен
ОК 5.	Стандартизація, сертифікація засобів та комплексів захисту інформації	6	екзамен
ОК 6.	Проектування технічних засобів захисту інформації	6	екзамен/ КП
ОК 7.	Нормативно-правове забезпечення інформаційної безпеки	4	залік
ОК 8.	Управління мережевою безпекою	5	залік
Загальний обсяг обов'язкових компонент:		37	
Вибіркові компоненти ОП			
ВБ 1.	Забезпечення безперервності бізнесу	4	залік
ВБ 2	Методологічні засади кібербезпеки	4	залік
ВБ 3.	Методи моделювання та оптимізації процесів в сфері захисту інформації	4	екзамен
ВБ 4.	Технології безпеки web-ресурсів	4	екзамен
ВБ 5.	Аудит та управління інцидентами інформаційної безпеки	5	екзамен
ВБ 6.	Технології безпеки бездротових і мобільних мереж	5	екзамен
ВБ 7.	Об'єктно-орієнтоване програмування	5	екзамен
ВБ 8.	Технології IoT та блокчейн	5	екзамен
ВБ 9.	Безпека в хмарних технологіях	5	екзамен
ВБ 10.	Інформаційно-психологічне протиборство	5	екзамен
Загальний обсяг вибіркових компонент:		23	
ОК 9.	Переддипломна практика	11	
ОК 10.	Підготовка до кваліфікаційної роботи	19	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90	

2.2. Структурно-логічна схема ОП

Послідовність навчальної діяльності здобувача за денною формою навчання:

Семестр	Види навчальної діяльності
I 30 кр.	Дисципліни загальної та професійної підготовки: ОК2 (2 кр.), ОК3 (5 кр.), ОК 4 (4кр.), ОК5 (6 кр.), ОК7 (4 кр.), ОК8 (5кр.). ВБ 3/ ВБ 4 (4 кр.)
II 30 кр.	Дисципліни загальної та професійної підготовки: ОК1 (3 кр.), ОК2 (2 кр.), ОК6 (6 кр.) ВБ1./ВБ2 (4кр.), ВБ 5/ ВБ 6 (5 кр.), ВБ 7/ВБ 8 (5 кр.), ВБ 9/ ВБ 10 (5 кр.)
III 30 кр.	ОК 9. Переддипломна практика (11 кр.), ОК 10. Підготовка до кваліфікаційної роботи (19 кр.).

3. Форма атестації здобувачів вищої освіти

Атестація здійснюється у формі публічного захисту випускної кваліфікаційної роботи.

На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання.

До атестації допускаються студенти, які виконали всі вимоги програми підготовки.

4.Матриця відповідності програмних компетентностей компонентам освітньої програми

Обов'язкові компоненти

	ОК 1.	ОК 2.	ОК 3.	ОК 4.	ОК 5.	ОК 6.	ОК 7.	ОК 8.	ОК 9.	ОК 10.
КЗ 1.	+	+	+	+		+	+	+	+	+
КЗ 2.		+	+	+	+	+	+	+	+	+
КЗ 3.		+		+		+	+		+	+
КЗ 4.			+	+	+	+	+	+	+	+
КЗ 5.	+		+	+	+	+	+	+	+	+
КЗ 6.	+									
КФ 1.			+		+		+			
КФ 2.			+			+		+		+
КФ 3.								+		
КФ 4.					+					
КФ 5.								+		+
КФ 6.								+		
КФ 7.							+			
КФ 8.				+	+	+	+			

4.Матриця відповідності програмних компетентностей компонентам освітньої програми

Вибіркові компоненти

	ВБ 1.	ВБ 2.	ВБ 3.	ВБ 4.	ВБ 5.	ВБ 6.	ВБ 7.	ВБ 8.	ВБ 9.	ВБ 10.
КЗ 1.	+	+	+	+	+	+	+	+	+	+
КЗ 2.	+	+	+	+	+	+	+	+	+	+
КЗ 3.			+							
КЗ 4.			+	+	+	+	+	+	+	+
КЗ 5.	+	+	+		+		+	+		+
КЗ 6.										
КФ 1.					+					
КФ 2.	+			+			+	+	+	
КФ 3.					+	+	+		+	
КФ 4.	+	+			+					
КФ 5.					+	+				+
КФ 6.					+					
КФ 7.			+		+		+			
КФ 8.			+				+	+		

5.Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми (обов'язкові дисципліни)

	ОК 1.	ОК 2.	ОК 3.	ОК 4.	ОК 5.	ОК 6.	ОК 7.	ОК 8.	ОК 9.	ОК 10.
ПРН 1		+		+		+	+			
ПРН 2				+		+	+	+	+	+
ПРН 3		+	+	+	+	+	+	+	+	+
ПРН 4			+		+	+	+		+	+
ПРН 5	+			+		+	+		+	+
ПРН 6	+		+		+		+	+		
ПРН 7					+			+		
ПРН 8					+			+		
ПРН 9						+		+		
ПРН 10					+					
ПРН 11								+		
ПРН 12							+			
ПРН 13								+		
ПРН 14	+						+			

5.Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми (вибіркові дисципліни)

	ВБ 1.	ВБ 2.	ВБ 3.	ВБ 4.	ВБ 5.	ВБ 6.	ВБ 7.	ВБ 8.	ВБ 9.	ВБ 10.
ПРН 1			+							
ПРН 2	+		+	+	+	+	+	+	+	+
ПРН 3	+	+	+	+	+	+	+	+	+	+
ПРН 4	+		+		+	+	+	+		+
ПРН 5			+				+	+		+
ПРН 6		+			+					
ПРН 7	+			+	+					
ПРН 8	+				+	+		+	+	
ПРН 9	+					+		+		
ПРН 10	+	+	+		+					
ПРН 11	+				+	+		+		
ПРН 12					+					
ПРН 13	+				+					
ПРН 14										