Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна

Введено в дію наказом від « 08 » 05 2020 р.
№ 0202-1/164

Ректор _____ Віль БАКІРОВ

« 08 » 05 2020 р.

Освітньо-професійна програма

Безпека інформаційних і комунікаційних систем

Спеціальність 125- Кібербезпека

(шифр, назва спеціальності)

Другий (магістерський) рівень вищої освіти

Затверджено вченою радою університету “ 27 ” 04 2020 року, протокол № 8.

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

1.1. Вчена рада факультету/інституту: протокол №_8_ від «_17_»_03_2020р.

Голова Вченої ради
факультету комп'ютерних наук Валентин ЛАЗУРИК

1.2. Методична комісія факультету/інституту:
протокол №_6_ від «_17_»_02_2020р.
Голова методичної комісії
факультету комп'ютерних наук Анатолій БЕРДНИКОВ

1.3.Кафедра: протокол №_6_ від «_15_»_01_2020 р.

Завідувач кафедри безпеки
інформаційних систем і технологій Сергій РАССОМАХІН

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Прізвище, ім’я, по батькові	Найменування посади (для сумісників – місце основної роботи, посада)	Науковий ступінь, вчене звання, за якою кафедрою (спеціальністю) присвоєно
Керівник робочої групи		
Єсін Віталій Іванович	Професор кафедри безпеки інформаційних систем і технологій	Доктор технічних наук (05.13.06 - Інформаційні технології), доцент за кафедрою спец. дисциплін
Члени робочої групи		
Рассомахін Сергій Геннадійович	Завідувач кафедри безпеки інформаційних систем і технологій	Доктор технічних наук (05.13.06 - Інформаційні технології), доцент за кафедрою автоматизованих систем управління
Кошман Сергій Олександрович	Професор кафедри безпеки інформаційних систем і технологій	Доктор технічних наук (05.13.05 – Комп’ютерні системи та компоненти), доцент за кафедрою автоматизації та комп'ютерно-інтегрованих технологій
Колованова Євгенія Павлівна	Доцент кафедри безпеки інформаційних систем і технологій	Кандидат технічних наук (05.13.21)

При розробці Програми враховані вимоги Освітнього стандарту спеціальності 125-«Кібербезпека» для першого (бакалаврського) рівня освіти, що погоджено рішенням Національного агентства із забезпечення якості вищої освіти від 22 травня 2017 р. № 72 та затверджено Наказом МОН України № 1074 від 04.10.2018 р. та робочого проекту стандарту для другого магістерського рівня.

1. Профіль освітньої програми «Безпека інформаційних і комунікаційних систем»

зі спеціальності 125 – Кібербезпека

1 – Загальна інформація	
Ступінь вищої освіти та назва кваліфікації	Другий (магістерський) рівень, магістр з кібербезпеки, безпека інформаційних і комунікаційних систем
Тип диплому та обсяг освітньої програми	90 кредитів
Офіційна назва програми	Безпека інформаційних і комунікаційних систем
Наявність акредитації	Первинна у 2014 році
Цикл/рівень	НРК України – 7 рівень, FQ – EHEA – другий цикл, QF – LLL – 7 шостий рівень
Передумови	Наявність першого (бакалаврського) рівня вищої освіти
Мова викладання	державна
Термін дії освітньої програми	5 років
Інтернет-адреса постійного розміщення опису освітньої програми	http://www-csd.univer.kharkov.ua/standarti-osviti/
2 - Мета освітньої програми	
Мета програми	Визначення основних компонент, програмних компетентностей та форм атестації випускників.
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності)**)**	12 – Інформаційні технології; 125 – Кібербезпека.
Орієнтація освітньої програми	Наукова, фундаментально-професійна.
Основний фокус освітньої програми та спеціалізації	Безпека інформаційно-комунікаційних систем і технологій
Особливості програми	Підготовка професіоналів, здатних розробляти, використовувати і впроваджувати технології інформаційної та/або кібербезпеки в інформаційно-комунікаційних системах.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	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.
Подальше навчання	Можливість продовжити навчання за освітньою програмою ступеня доктора філософії.
5 – Викладання та оцінювання	
Викладання та навчання	Денна форма навчання. Лекції, лабораторні роботи, семінари, практичні заняття, самостійна робота на основі підручників та конспектів, консультації з викладачами, виробнича та переддипломна практика, написання магістерської роботи.
Оцінювання	Письмові екзамени, звіти з лабораторних та практичних робіт, курсові роботи, поточний контроль. За 100 бальною та 4 (2)-ох рівневою національною шкалою
6 – Програмні компетентності	
Інтегральна компетентність	-Здатність до самостійної науково-дослідної діяльності в галузі кібербезпеки (аналіз, співставлення, систематизація, абстрагування, моделювання, перевірка достовірності даних, прийняття рішень та ін.), готовність генерувати та використовувати нові ідеї; - методологічні знання і дослідницькі уміння, що забезпечують виконання завдань науково-дослідної, науково-педагогічної, управлінської і інноваційної діяльності при удосконаленні безпеки інформаційних і комунікаційних систем; - здатність протягом життя самостійно вчитися, забезпечувати особистісний та професійний розвиток.
Загальні компетентності	**КЗ 1**. Готовність використати сучасні досягнення науки і передових технологій. **КЗ 2**. Здатність застосовувати знання у практичних ситуаціях; 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 науково-технічні завдання за професійним спрямуванням; здатність планувати та здійснювати власне наукове дослідження, присвячене суттєвій проблемі сучасної науки у галузі інформаційно-комунікаційних технологій. **КЗ 5**. Здатність до пошуку, оброблення та аналізу інформації; готовність представляти результати досліджень у вигляді звітів і публікацій на державній та одній з іноземних мов; здатність користуватися нормативною та законодавчою базою в сфері інтелектуальної власності. **КЗ 6**. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні;

	КЗ 7. Розуміти глобальні проблеми сучасності; володіти здатністю зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. **КЗ 8.** Здатність до викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційно-комунікаційних технологій; здатність розробляти методичні матеріали, що використовуються в навчальному процесі.
Фахові компетентності	**КФ 1**. Здатність розуміти і аналізувати напрями розвитку розподілених інформаційно-комунікаційних систем і мереж, загальної теорії побудови математичних моделей і їх реалізації, теорії і практики керівництва проектами зі створення захищених розподілених інформаційних ресурсів. **КФ 2**. Здатність виконувати роботи з проектування складних комплексів засобів кібербезпеки і управління безпекою інформаційних і комунікаційних систем відповідно до сфери їх застосування. **КФ 3**. Здатність здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення кібербезпеки. **КФ 4**. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. **КФ 5.** Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. **КФ 6.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. **КФ 7.** Здатність організувати роботу відповідно до вимог безпеки життєдіяльності й охорони праці; знання наукових та практичних основ адміністрування та експлуатації захищених інформаційних і комунікаційних систем; **КФ 8**. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації

	встановленої політики інформаційної та/або кібербезпеки. **КФ 9**. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. **КФ 10**. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) **КФ 11**. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **КФ 12**. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
7 – Програмні результати навчання	
Програмні результати навчання	**ПРН 1.** Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. **ПРН 2.** Застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. **ПРН 3**. Вміння аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. **ПРН 4**. Вміння розробляти проектну документацію, програми та методики випробувань, оцінці якості програмних продуктів, організовувати тестування та налагодження програмно-технічних комплексів та засобів захисту інформаційних і комунікаційних систем. **ПРН 5**. Впровадження в інформаційні і комунікаційні системи сучасні методи забезпечення кібербезпеки відповідно до вимог вітчизняних та міжнародних стандартів. **ПРН 6**. Володіння науковими та практичними методами створення систем моніторингу якості ПЗ та кібербезпеки в інфокомунікаційних системах та мережах **ПРН 7**. Володіння методологією обґрунтування вибору, реалізації й аналізу криптографічних механізмів та систем захисту інформаційних і комунікаційних систем. **ПРН 8**. Навики здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення безпеки бездротових кіберсистем.

	ПРН 9. Вміння здійснювати та детально обґрунтовувати вибір архітектури інфраструктури відкритих ключів, що проектується. **ПРН 10**. Володіння науково-організаційними основами проведення аудиту якості та безпеки кіберсистем. **ПРН 11**. Застосовування основних методів, принципів та засобів захисту інформації при організації безпеки банківських систем. **ПРН 12**. Вміння обґрунтовувати доцільність та забезпечувати ефективність взаємовідносин з відповідними зовнішніми організаціями щодо забезпечення економічної безпеки. **ПРН 13**. Аналізувати, аргументувати, приймати рішення при розв'язанні складних науково-технічних задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. **ПРН 14**. Розробка пропозиції та здійснення впровадження нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. **ПРН 15 В**иконання комплексний аналіз та декомпозицію інформаційно-телекомунікаційних систем, виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; **ПРН 16.** Розроблення та оцінювати адекватність моделі загроз та порушника, аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. **ПРН 17.** Використання сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; володіння методами безпечного програмування. **ПРН 18 Р**еалізація комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативно-правових документів. **ПРН 19.** Вміння реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних системах. **ПРН 20.** Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом.
8 – Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового забезпечення	Викладання фахових дисциплін забезпечує професорсько-викладацький склад кафедри: 9 докторів та 8 кандидатів наук.

Специфічні характеристики матеріально-технічного забезпечення	Для навчання використаються 8 комп'ютерних класів та навчальна лабораторія факультету комп'ютерних наук, навчально-науковий центр сертифікації ключів ЕЦП, виробнича та переддипломна практика здійснюється на базі ФКН та 3-ох науково-виробничих підприємствах.
Специфічні характеристики інформаційного та навчально-методичного забезпечення	Використається навчальний фонд бібліотеки ХНУ, ПЗ дистанційних форм навчання, підручники та навчальні посібники розробки кафедри та провідних світових університетів.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом ім. В. Н. Каразіна та іншими університетами України. Допускаються індивідуальні угоди про академічну мобільність для навчання та проведення досліджень в університетах та наукових установах України. До керівництва науковою роботою здобувачів можуть бути залучені провідні фахівці університетів України на умовах індивідуальних договорів. Кредити, отримані в інших університетах України, перезараховуються відповідно до довідки про академічну мобільність.
Міжнародна кредитна мобільність	Відповідно до «Стратегії гармонізації державного управління країн ЄС та Східного Партнерства», що підписана 28 країнами Європи, в тому числі й Україною, передбачено формування єдиного освітнього простору країн ЄС та Східного Партнерства. Даною загальноєвропейською стратегією передбачено й впровадження міжнародних програм студентського обміну та програм подвійних дипломів між найбільшими українськими університетами та провідними університетами ЄС. Харківський національний університет ім. В. Н. Каразіна є активним учасником даного міжнародного процесу. Міжнародна кредитна мобільність може здійснюватися також на основі двосторонніх договорів між Харківським національним університетом ім. В. Н. Каразіна та закладами вищої освіти зарубіжних країн-партнерів.
Навчання іноземних здобувачів вищої освіти	На загальних умовах. Іноземні здобувачі вищої освіти, що реалізують право на академічну мобільність в рамках договорів про співробітництво між Харківським національним університетом ім. В. Н. Каразіна та іноземними вищими навчальними закладами-партнерами, можуть бути зараховані на навчання за рахунок коштів міжнародних програм та організацій або за рахунок коштів фізичних або юридичних осіб.

2. Перелік компонент освітньо-професійної /наукової 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 підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК 1.	Глобальні проблеми сучасності	3	Залік
ОК 2.	Математичні основи проектування та оптимізації інформаційно-комунікаційних систем (Курс. р.)	11	Екзамен (2)
ОК 3.	Розробка та супровід проблемно-орієнтованих програмних систем (Курс. р.)	7	Екзамен (2)
ОК 4.	Методологія і організація наукових досліджень (Курс. р.)	3	Залік
ОК 5.	Теорія надійності програмних і технічних систем	5	Екзамен
ОК 6.	Стандартизація в сфері кібербезпеки	4	Екзамен
ОК 7.	Науково-дослідна практика	10	Залік
ОК 8.	Переддипломна практика	10	Залік
ОК 9.	Виконання кваліфікаційної роботи магістра	10	Захист
Загальний обсяг обов'язкових дисциплін		65	
Вибіркові компоненти ОП*			
Вибірковий блок 1			
ВБ 1.1.	Основи патентознавства	3	Залік
ВБ 1.2.	Чинники успішного працевлаштування за фахом	3	Залік
ВБ 1.3.	Криптографічні методи в кібербезпеці (Курс. р.)	6	Екзамен (2)
ВБ 1.4.	Безпека бездротових мереж	7	Екзамен
1	2	3	4
ВБ 1.5.	Теорія розподілених інформаційних ресурсів, захист баз даних та знань (Курс. р.)	6	Екзамен
Вибірковий блок 2			
ВБ 2.1.	Охорона інтелектуальної власності	3	Залік
ВБ 2.2.	Сучасні тенденції ринку ІТ	3	Залік
ВБ 2.3.	Моніторинг та аудит безпеки та якості інформаційних систем та програмного забезпечення	6	Екзамен
ВБ 2.4.	Основи тестування програмного забезпечення	7	Екзамен
ВБ 2.5.	Моделі, методи та програмно-апаратні засоби комплексу захисту інформації хмарних сервісів (Курс. р.)	6	Екзамен
Загальний обсяг вибіркових дисциплін		25	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90	

2.2 Структурно-логічна схема ОП

Рік навчання	1-й		2-й	
Семестр	1	2	3	4
ОК 1.				
ОК 2.				
ОК 3.				
ОК 4.				
ОК 5.				
ОК 6.				
ОК 7.				
ОК 8.				
ОК 9.				
ВБ 1.1.				
ВБ 1.2.				
ВБ 1.3.				
ВБ 1.4.				
ВБ 1.5.				
ВБ 2.1.				
ВБ 2.2.				
ВБ 2.3.				
ВБ 2.4.				
ВБ 2.5.				

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється екзаменаційною комісією відповідно до вимог цього стандарту після виконання студентом навчального плану. На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за даною програмою. Термін проведення атестації визначається навчальним планом та графіком освітнього процесу. Атестація здійснюється у формі публічного захисту кваліфікаційної магістерської роботи. До атестації допускаються студенти, які виконали всі вимоги програми.
Вимоги до кваліфікаційної роботи/проекту	Кваліфікаційний робота має передбачати розв’язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки. Кваліфікаційний проект/ робота має бути перевірений на плагіат. Оприлюднення на сайті.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

		КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КЗ 8	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ	КФ	КФ
ОК 1.	Глобальні проблеми сучасності	+		+			+	+	+												
ОК 2.	Математичні основи проектування та оптимізації інформаційно-комунікаційних систем	+			+				+	+	+	+							+		
ОК 3.	Розробка та супровід проблемно-орієнтованих програмних систем	+	+		+					+	+				+	+			+		
ОК 4.	Методологія і організація наукових досліджень	+			+										+				+		
ОК 5.	Теорія надійності програмних і технічних систем											+				+					+
ОК 6.	Стандартизація в сфері кібербезпеки	+	+						+				+			+	+	+	+		+
ОК 7.	Науково-дослідна практика	+		+	+	+			+			+			+						
ОК 8.	Переддипломна практика	+		+					+			+									
ОК 9.	Виконання кваліфікаційної роботи магістра	+	+	+					+			+									
ВБ 1.1.	Основи патентознавства					+													+		
ВБ 1.2.	Чинники успішного працевлаштування за фахом		+			+			+												
ВБ 1.3.	Криптографічні методи в кібербезпеці	+	+							+		+					+	+			+
ВБ 1.4.	Безпека бездротових мереж		+							+				+							+
ВБ 1.5.	Теорія розподілених інформаційних ресурсів, захист баз даних та знань		+									+		+						+	
ВБ 2.1.	Охорона інтелектуальної власності					+													+		
ВБ 2.2.	Сучасні тенденції ринку ІТ		+									+			+					+	
ВБ 2.3.	Моніторинг та аудит безпеки та якості інформаційних систем та програмного забезпечення		+									+					+				
ВБ 2.4.	Основи тестування програмного забезпечення	+	+									+		+							
ВБ 2.5.	Моделі, методи та програмно-апаратні засоби комплексу захисту інформації хмарних сервісів		+									+		+			+			+	

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

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ВБ 1.1	ВБ 1.2	ВБ 1.3	ВБ 1.4	ВБ 1.5	ВБ 2.1	ВБ 2.2	ВБ 2.3	ВБ 2.4	ВБ 2.5
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									+	+	+			+	+	+		+	
ПРН 15				+		+						+	+				+		+
ПРН 16					+			+	+					+				+	
ПРН 17			+					+	+			+		+			+	+	
ПРН 18				+				+	+				+	+				+	+
ПРН 19								+	+			+		+			+	+	
ПРН 20						+		+	+				+	+				+	+