МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В.Н. КАРАЗІНА

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ»

Другий (магістерський) рівень вищої освіти

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 - Кібербезпека та захист інформації

ЗАТВЕРДЖЕНО
Вченою радою університету
протокол від _____ № _____

Введено в дію з _____
наказ від _____ № _____

Проректор з науково-педагогічної роботи
Олександр ГОЛОВКО
_____

ХАРКІВ–2024

ЛИСТ ПОГОДЖЕННЯ ОПП

Науково-методичною радою університету
протокол від _____ № _____
Голова НМР
_____ **Олександр ГОЛОВКО**

Вчена рада факультету комп'ютерних наук
протокол від _____ № _____
Заступник Голови Вченої ради факультету
_____ **Олена ТОЛСТОЛУЗЬКА**

Методична комісія факультету комп'ютерних наук
протокол від _____ № _____
Голова методичної комісії факультету
_____ **Лариса ВАСИЛЬЄВА**

Кафедра безпеки інформаційних систем і технологій
протокол від _____ № _____
в.о. завідувача кафедри
_____ **Ольга МЕЛКОЗЬОРОВА**

ПЕРЕДМОВА

При розробці проекту Програми враховані вимоги:

– Освітнього стандарту спеціальності 125-« Кібербезпека та захист інформації» для другого (магістерського) рівня освіти, що погоджено рішенням Національного агентства із забезпечення якості вищої освіти, протокол від 23.02.2021 р. № 3, та Затверджено і введено в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.
– Закон України "Про вищу освіту" – http://zakon4.rada.gov.ua/laws/http://zakon4.rada.gov.ua/laws/show/1556-18.
– Закон України "Про освіту" – http://zakon5.rada.gov.ua/laws/show/2145-19.
– Національний класифікатор України: "Класифікатор професій" ДК 003:2010.
– Національна рамка кваліфікацій – http://zakon4.rada.gov.ua/laws/show/ https://zakon.rada.gov.ua/laws/show/1341-2011-%D0%BF#Text.
– Перелік галузей знань і спеціальностей – http://zakon4.rada.gov.ua/http://zakon4.rada.gov.ua/ laws/show/266-2015-plaws/show/266- 2015-п.
– Методичні рекомендації щодо розроблення стандартів вищої освіти.
– Затверджено Наказом Міністерства освіти і науки України від 01.06.2017 р. № 600 (у редакції наказу Міністерства освіти і науки України від 30.04.2020 р. № 584 – https://mon.gov.ua/storage/app/media/vyshcha/naukovo-metodychna_rada/2020metod- rekomendacziyi.docx

Розроблено робочою групою у складі:

Прізвище, ім’я, по батькові	Найменування посади	Науковий ступінь, вчене звання, за якою кафедрою (спеціальністю) присвоєно
Керівник робочої групи		
Єсін Віталій Іванович	Професор кафедри безпеки інформаційних систем і технологій, гарант програми	Доктор технічних наук (05.13.06 - Інформаційні технології), доцент за кафедрою автоматизованих систем управління
Члени робочої групи		
Кузнецов Олександр Олександрович	Професор кафедри безпеки інформаційних систем і технологій	Доктор технічних наук (05.13.21 – системи захисту інформації), професор за спеціальністю 20.02.12 - військова кібернетика, системи управління та зв'язок
Сватовський Ігор Іванович	Доцент кафедри безпеки інформаційних систем і технологій	Кандидат технічних наук, старш.наук.співр.
Мелкозьорова Ольга Михайлівна	Доцент кафедри безпеки інформаційних систем і технологій	Кандидат технічних наук (05.13.21 – системи захисту інформації)
Колованова Євгенія Павлівна	Доцент кафедри безпеки інформаційних систем і технологій	Кандидат технічних наук (05.13.21 – системи захисту інформації)

1. Профіль освітньої програми «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 – Кібербезпека та захист інформації

1–Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Харківський національний університет імені В.Н. Каразіна, кафедра безпеки інформаційних систем і технологій
Ступінь вищої освіти та назва освітньої кваліфікації	Другий (магістерський) рівень, Магістр з кібербезпеки та захисту інформації, безпеки інформаційних і комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання: денна форма – 1 роки 4 місяці.
Офіційна назва програми	Безпеки інформаційних і комунікаційних систем
Наявність акредитації	2017 рік
Цикл/рівень	НРК України - 8 рівень, FQ-EHEA - другий цикл, QF-LLL - 7 рівень
Передумови	Для здобуття освітнього ступеня магістра можуть вступати особи, які здобули перший (бакалаврський) рівень вищої освіти
Мова викладання	Українська
Термін дії освітньої програми	з 2024 до 2025 року
Інтернет - адреса постійного розміщення опису освітньої програми	http://www-csd.univer.kharkov.ua/navchannya/standarti-osviti/osviti-programi/
2 - Мета освітньої програми	
Мета програми	Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної безпеки для розв'язання практичних завдань кібербезпеки та профілактики кіберзагроз
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності)**)**	12 – Інформаційні технології;125 – Кібербезпека та захист інформації.
Орієнтація освітньоїпрограми	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 працевлаштуваннята 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 освітньо-науковоюпрограмою доктора філософії.
5 – Викладання та оцінювання	
Викладання та навчання	Вивчення компонент освітньої (професійної) програми передбачається у формі проведення навчальних занять, організації самостійної роботи здобувачів вищої освіти, практичної підготовки та контрольних заходів. Навчальні заняття проводиться у виді: лекційних курсів, зокрема мультимедійних, семінарських, практичних, індивідуальних, лабораторних занять, консультацій тощо.
Оцінювання	Усні, письмові екзамени та заліки, комп’ютерне і письмове тестування, презентації, захист курсових робіт, матеріалів практики, атестація За 100 бальною та чотирьох (дво)рівневою національною шкалою
6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційноїбезпеки та/або кібербезпеки.
Загальні компетентності	**КЗ 1**. Готовність використати сучасні досягнення науки іпередових технологій. **КЗ 2**.Здатність застосовувати знання у практичних ситуаціях; знання та розуміння предметної області та розуміння професії. **КЗ 3**. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності), здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **КЗ 4**. Здатність проводити дослідження на відповідному рівні. 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 абстрактного мислення, аналізу та синтезу. 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 оцінювати та забезпечувати якість виконуваних робіт. 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 обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. 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 розробляти, впроваджувати та аналізувати нормативні документи, положення,

	інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. Здатність виконувати роботи з проектування складних комплексів засобів кібербезпеки і управління безпекою інформаційних і комунікаційних систем відповідно до сфери їх застосування. **КФ 3**.Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. Здатність здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпеченнякібербезпеки. **КФ 4**.Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів тавимог. **КФ 5.**Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. **КФ 6.**Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії іполітики інформаційної безпеки та/або кібербезпеки організації. **КФ 7.**Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. **КФ 8**. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації наоб'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики

	інформаційної безпеки та/або кібербезпеки організації. **КФ 9**. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації вцілому. **КФ 10**. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. **КФ 11**. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність. **КФ 12**. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційноюта/або кібербезпекою.
7 – Програмні результати навчання	
Програмні результати навчання	**ПРН 1.**Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпекита/або кібербезпеки. **ПРН 2.**Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. **ПРН3**. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. **ПРН 4**. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. **ПРН 5**. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико- математичних наук, а також

	розвитку технологій створення та використання спеціалізованогопрограмного забезпечення. **ПРН 6**. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. **ПРН 7**. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. **ПРН 8**. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. **ПРН 9**Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. **ПРН 10**. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. **ПРН 11**. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. **ПРН 12**. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснюватипроцедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. **ПРН 13**. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. **ПРН 14**. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

	ПРН 15Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. **ПРН 16.**Приймати обґрунтовані рішення з організаційно- технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. **ПРН 17**Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. **ПРН 18**Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. **ПРН 19.** Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. **ПРН 20.** Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/абокібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. **ПРН 21.**Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. **ПРН22.** Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувативисновки. **ПРН23.** Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

8 – Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового забезпечення	Викладання фахових дисциплін забезпечує професорсько-викладацький склад кафедри: 6 докторів та 8 кандидатів наук, які є штатними співробітниками університету.
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 університету, ПЗ дистанційних форм навчання, підручники та навчальні посібники розробки кафедри та провідних світових університетів.
9 – Академічна мобільність	
Національна кредитна мобільність	Студенти мають можливість здійснювати перехід до інших ВНЗ та/або спеціальностей (згідно до положень Закону про освіту та відповідних рішень ВНЗ) з урахуванням накопиченого обсягу кредитів навчання.
Міжнародна кредитна мобільність	Студенти мають можливість здійснювати навчання в ВНЗ інших країн у відповідності з домовленостями університетів в рамках міжнародних програм співробітництва та академічної мобільності.
Навчання іноземних здобувачів вищої освіти	Можливим є навчання іноземних студентів за даною програмою з використанням державної, англійської або інших мов викладання.

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 рактики, 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	Іспит (2)
ОК 3.	Розробка та супровід проблемно-орієнтованих програмних систем (Курс.р.)	7	Іспит (2)
ОК 4.	Методологія і організація наукових досліджень (Курс. р.)	3	Залік
ОК 5.	Теорія надійності програмних і технічних систем	5	Іспит
ОК 6.	Стандартизація в сфері кібербезпеки	4	Іспит
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	Іспит (2)
ВБ 1.4.	Безпека бездротових мереж	7	Іспит
ВБ 1.5.	Теорія розподілених інформаційних ресурсів, захист баз даних та знань (Курс.р.)	6	Іспит
Вибірковий блок 2			
ВБ 2.1.	Охорона інтелектуальної власності	3	Залік

ВБ 2.2.	Сучасні тенденції ринку IT	3	Залік
ВБ 2.3.	Моніторинг та аудит безпеки та якості інформаційних систем та програмного забезпечення	6	Іспит
ВБ 2.4.	Основи тестування програмного забезпечення	7	Іспит
ВБ 2.5.	Моделі, методи та програмно-апаратні засоби комплексу захисту інформаціїхмарних сервісів (Курс. р.)	6	Іспит
Загальний обсяг вибіркових дисциплін		25	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ		90	

2.2 Структурно-логічна схема ОП

Рік навчання	1-й		2-й	
Семестр	1	2	3	
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 вищоїосвіти	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 таграфіком освітнього процесу. Атестація здійснюється у формі публічного захисту кваліфікаційної магістерської роботи. До атестації допускаються студенти, які виконали всі вимогипрограми.
Вимоги до кваліфікаційної роботи/проекту	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозиторії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

		КЗ	КЗ	КЗ	КЗ	КЗ	КЗ	КЗ	КЗ	КФ	КФ	КФ	КФ	КФ	КФ	КФ	КФ	КФ	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 IT		+									+			+					+	
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	ВБ2.2	ВБ2.3	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						+		+	+				+	+				+	+
ПРН 21		+	+				+	+		+	+		+			+			+
ПРН 22	+			+		+			+	+		+			+		+	+	
ПРН 23	+				+	+		+		+	+		+			+	+		