ПРОЕКТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖЕНО

Вченою радою ХНЕУ ім. С. Кузнеця
Протокол № ___ від ___.___.2020 р.
Голова Вченої ради

Ректор_____В. С. Пономаренко

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

РІВЕНЬ ВИЩОЇ ОСВІТИ	**Другий (магістерський) рівень**
СТУПІНЬ ВИЩОЇ ОСВІТИ	**Магістр**
ГАЛУЗЬ ЗНАНЬ	**12 Інформаційні технології**
СПЕЦІАЛЬНІСТЬ	**125 “Кібербезпека”**

ХАРКІВ, 2020

І. Преамбула

1. РОЗРОБЛЕНО

Методичною комісією Харківського національного економічного університету імені Семена Кузнеця.

Голова методичної комісії:

Пономаренко В.С., д.е.н., проф., ректор ХНЕУ імені С. Кузнеця.

2. ЗАТВЕРДЖЕНО ТА НАДАНО ЧИННОСТІ

Освітньо-професійна програма другого (магістерського) рівня галузі знань 12 Інформаційні технології, спеціальності 125 “Кібербезпека” затверджена та введена в дію Наказом ректора Харківського національного економічного університету імені Семена Кузнеця від ___.___.2020 р. № ____ у відповідності до рішення вченої ради університету від ___.___.2020 р. Протокол № ____ .

3. РОЗРОБНИКИ ОПП

Євсеєв Сергій Петрович, доктор технічних наук, завідувач кафедри кібербезпеки та інформаційних технологій.

Алексієв Володимир Олегович, доктор технічних наук, професор кафедри кібербезпеки та інформаційних технологій.

Мілов Олександр Володимирович, кандидат технічних наук, професор кафедри кібербезпеки та інформаційних технологій.

Ковтун Владислав Юрійович, кандидат технічних наук, технічний директор ТОВ “Сайфер БІС”.

Кравченко Павло Олександрович, співзасновник “Distributed Lab”.

Макаренко Антон Олегович, студент 4 курсу першого (бакалаврського) рівня вищої освіти за спеціальністю 125 “Кібербезпека”.

ІІ. Загальна характеристика

Рівень вищої освіти	Другий (магістерський) рівень НРК України – 8 рівень, FQ-EHEA – другий цикл, QF-LLL – 7 рівень
Ступінь вищої освіти	Магістр
Галузь знань	12 Інформаційні технології
Спеціальність	125 “Кібербезпека”
Освітня програма	“Кібербезпека”
Освітня кваліфікація	Магістр з кібербезпеки за освітньо-професійною програмою “Кібербезпека”
Кваліфікація в дипломі	Магістр з кібербезпеки за освітньо-професійною програмою “Кібербезпека”
Опис предметної області	**Об’єкти вивчення:** об’єкти інформатизації, включаючи комп’ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення складових безпеки інформації: інформаційна безпека, кібербезпека, безпека інформації; процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту; теоретичні та правові основи використання, принципи функціонування блокчейн технологій, обігу криптовалют. **Цілі навчання:** підготовка професіоналів, здатних використовувати і впроваджувати технології та застосовувати засоби інформаційної та/або кібербезпеки, які володіють механізмами забезпечення безпеки в децентралізованих системах, ефективними засобами обмежень ризиків створення та використання криптовалют, використання смартконтрактів. **Теоретичний зміст предметної області:** принципи формування систем забезпечення інформаційної та/або кібербезпеки; методи та засоби виявлення, управління та ідентифікації ризиків; загальні принципи та правила застосування криптографічних способів у блокчейн технології, методологічні основи розробки та функціонування блокчейн платформ, смартконтрактів, методи та механізми забезпечення безпеки в сучасних системах цифровій економіки. **Методи, методики та технології:** статистичні, якісні та кількісні методи/ методики оцінки поточного стану інформаційної безпеки; експертного оцінювання, математичного моделювання, прогнозування; інформаційно-комунікаційні технології, спеціальне програмне забезпечення; методи дослідницької діяльності та презентації результатів. **Інструменти та обладнання:** сучасне інформаційно-

	комунікаційне обладнання, Security Information and Event Management системи та програмні продукти: управління інформаційною безпекою (Security Information Management), та управління подіями безпеки (Security Event Management).
Академічні права випускників	Можливість продовження навчання на третьому (освітньо-науковому) рівні (доктор філософії) за спеціальністю “Кібербезпека”; отримання післядипломної освіти на споріднених та інших спеціальностях; підвищення кваліфікації.
Працевлаштування випускників	Магістр з кібербезпеки може працювати керівником підприємств, установ та організацій, керівним працівником апарату місцевих органів державної влади; керівником підрозділів комп’ютерних послуг; керівником проектів та програм; менеджером (управителем) систем з інформаційної безпеки; розробником комп’ютерних програм; викладачем університетів та вищих навчальних закладів; науковим співробітником (інформаційна аналітика); професіоналом в галузі інформації та інформаційні аналітики; науковим співробітником (електроніка, телекомунікації, проекти та програми), професіоналом з управління проектами та програмами

ІІІ. Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти

Обсяг освітньо-професійної програми підготовки магістра галузі знань 12 “Інформаційні технології” за освітньо-професійною програмою “Кібербезпека” спеціальності 125 “Кібербезпека” (бакалавр) – 90 кредитів ЄКТС.

Термін навчання:

денна форма – один рік 4 місяці;

заочна форма – один рік 4 місяці.

Обсяг кредитів ЄКТС для здобуття ступеня магістра зі спеціальності 125 Кібербезпека освітньо-професійна програма “Кібербезпека”

Цикли підготовки	**Кількість кредитів ECTS**
Освітньо-професійна програма магістра за циклами:	**90**
Цикл професійної підготовки	**90**
у т. ч.	
базові навчальні дисципліни	67 (74 %)
вибіркові навчальні дисципліни	23 (26 %)

Вибіркова складова освітньо-професійної програми складається з:

МАГ-МАЙНОР – умовна назва вибіркових дисциплін із загального переліку Університету (загальноуніверситетський пул) для освітньо-кваліфікаційного рівня магістр. Дисципліни **МАГ-МАЙНОР** є обов’язковими для вибору студентами і входять до загального обсягу кредитів ЄКТС за освітньо-професійною програмою підготовки магістрів.

Ідея дисциплін **МАГ-МАЙНОР** полягає у вільному виборі студентами магістратури дисциплін таких напрямків, які відображають його інтереси, вподобання та плани на майбутнє працевлаштування. Взяти участь у **МАГ-МАЙНОР** можуть усі факультети і кафедри університету. Індивідуальний план студента буде формуватися з найкращих на його думку навчальних дисциплін.

Загальний обсяг **МАГ-МАЙНОР** складає 20 кредитів ЄКТС (по 5 кредитів на дисципліну):

КОМПЛЕКСНИЙ ТРЕНІНГ. Головною метою комплексного тренінгу є формування у студентів навичок прийняття послідовних рішень щодо вибору механізмів забезпечення безпеки в сучасних обчислювальних мережах і системах, методів криптоаналізу щодо визначення рівня стійкості обраних криптосистем.

IV. Перелік компетентностей випускника

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 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. Здатність 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.
Спеціальні (фахові, предметні) компетентності	КФ 1. Здатність розробляти та впроваджувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. КФ 2. Здатність розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах (інформаційних, інформаційно-телекомунікаційних, автоматизованих). КФ 3. Здатність розробляти й впроваджувати систему менеджменту інформаційної безпеки та/або кібербезпеки організації, формувати стратегію і політики інформаційної безпеки різних рівнів на базі світових й вітчизняних стандартів з урахуванням кращих практик галузі інформаційних технологій та їх безпеки. КФ 4. Здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, безпеки інформаційних технологій (в т.ч. хмарних технологій та додатків), а також безпеки

	бізнес/операційних процесів з метою забезпечення функціонування інформаційно-комунікаційних систем згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ 5. Здатність розробляти та впроваджувати систему управління інформаційними активами (ресурсами), володіти методами теорії ризик менеджменту та процесних моделей, розробляти моделі загроз й моделі порушника, а також забезпечувати штатне функціонування системи інформаційної безпеки та/або кібербезпеки організації з використанням сучасних технологій. КФ 6. Здатність планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів установи, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ 7. Здатність аналізувати причини та наслідки збоїв або відмов функціонування інформаційних систем, що викликані реалізацією різного класу кіберінцидентів, а також розробляти й впроваджувати методи і заходи відновлення штатного функціонування інфраструктури організації в цілому. КФ 8. Здатність розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, а також систему аудиту і контролю функціонування інформаційно-комунікаційних систем та технологій (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ 9.Здатність розробляти та впроваджувати методи і заходи протидії кіберінцидентам, а також здійснювати процедури управління, контролю та розслідування, надавати рекомендації щодо попередження та аналізу кіберінцидентів. КФ 10. Здатність розробляти, впроваджувати, та супроводжувати бізнес/операційні процеси з використанням методів та засобів криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ 11. Здатність розробляти, впроваджувати і супроводжувати системи аудиту та моніторингу якості бізнес/операційних процесів інформаційно-комунікаційних систем та технологій, а також системи менеджменту інформаційної безпеки та/або кібербезпеки організації в цілому. КФ 12. Здатність проводити науково-освітню діяльність, розробляти та впроваджувати систему управління персоналом, а також проводити та планувати навчання працівників і наукові дослідження в сфері безпеки інформаційно-комунікаційних систем і технологій у відповідність вітчизняним та світовим стандартам галузі інформаційної безпеки та/або кібербезпеки.

З метою забезпечення кореляції визначених компетентностей з класифікацією компетентностей НРК використовується матриця відповідності визначених компетентностей та дескрипторів НРК, яка є інформаційним додатком (Таблиця 1 Пояснювальної записки).

V. Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання за спеціальністю 125 “Кібербезпека” освітньо-професійна програма “ Кібербезпека”

Результати навчання	ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат; ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки; ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому; ПРН-7 – виявляти, описувати та використовувати систему аналізу зв’язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства); ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних

	систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо); ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства); ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії;

	ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки; ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства); ПРН-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на підприємстві; ПРН-20 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

СТРУКТУРА ПРОГРАМИ ПІДГОТОВКИ МАГІСТРІВ

Галузь знань 12 “Інформаційні технології”,
спеціальність 125 “Кібербезпека”
освітньо-професійна програма “Кібербезпека”

Складові освітньо-професійної програми		Загальна кількість		Форма контролю
		кредитів ЄКТС	годин	
Цикл професійної підготовки				
БАЗОВА СКЛАДОВА				
Б 1	ГОСПОДАРСЬКЕ ПРАВО	2	60	Залік
Б 2	АНГЛІЙСЬКА МОВА	2	60	Залік
Б 5	ПРЕЗЕНТАЦІЯ ТА ОБРОБКА ЗНАНЬ	3	90	Залік
Б 6	ПЕРЕДОВІ МЕТОДИКИ ПРОГРАМУВАННЯ	3	90	Екзамен
Б 7	БЕЗПЕКА ІНТЕРНЕТ РЕЧЕЙ	3	90	Залік
Б 8	РОЗШИРЕНА МЕРЕЖЕВА ТА ХМАРНА БЕЗПЕКА	3	90	Екзамен
Б 9	ЦИФРОВА КРИМІНАЛІСТИКА	4	120	Екзамен
Б 10	ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ТА ЕТИЧНИЙ ХАКІНГ	4	120	Екзамен
Б 11	ВЕБ-БЕЗПЕКА	3	90	Екзамен
Б 12	БЕЗДРОТОВА ТА МОБІЛЬНА БЕЗПЕКА	4	120	Екзамен
Б 13	ЗАХИСТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ	2	60	Залік
Б 14	МИСТЕЦТВО РЕДАГУВАННЯ ТА РИТОРИКА	2	60	Залік
НДП	НАУКОВО-ДОСЛІДНА ПРАКТИКА	2	60	Звіт
ПП	ПЕРЕДДИПЛОМНА ПРАКТИКА	12	360	Звіт
Д	ДИПЛОМНИЙ ПРОЕКТ	18	540	Дипломний проект
ВСЬОГО БАЗОВА СКЛАДОВА		**67**	**2010**	
ВИБІРКОВА СКЛАДОВА				
ММ1	ІНЖЕНЕРІЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ	5	150	Залік
ММ2	РОЗШИРЕНЕ АДМІНІСТРУВАННЯ СЕРВЕРНИХ СЕРВІСІВ	5	150	Залік
ММ3	БЕЗПЕКА СЕРВЕРНИХ СИСТЕМ	5	150	Залік
ММ4	БЕЗДРОТОВІ ТА ОПТИЧНОВОЛОКОННІ МЕРЕЖІ	5	150	Залік
Т	ТРЕНІНГ-КУРС:БЛОКЧЕЙН: МАТЕМАТИЧНІ ПРОБЛЕМИ ТА ЗАСТОСУНКИ або ТРЕНІНГ-КУРС: КРИПТОГРАФІЯ ТА КРИПТОАНАЛІЗ	3	90	Залік
ВСЬОГО ВИБІРКОВА СКЛАДОВА		**23**	**690**	
ЗАГАЛЬНА КІЛЬКІСТЬ		**90**	**2700**	

VI. Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація за спеціальністю здійснюється екзаменаційною комісією відповідно до вимог стандарту вищої освіти після виконання студентом навчального плану у формі: публічного захисту кваліфікаційної роботи магістра за спеціальністю 12 Інформаційні технології, освітньо-професійною програмою "Кібербезпека"(денна форма) або єдиного кваліфікаційного іспиту за спеціальністю у порядку, визначеному Кабінетом Міністрів України (заочна форма). До атестації допускаються студенти, які виконали всі вимоги освітньої програми та навчального плану. Результати атестації визначаються оцінками за національною шкалою: "відмінно", "добре", "задовільно", "незадовільно".
Вимоги до заключної кваліфікаційної роботи	Харківський національний економічний університет імені Семена Кузнеця розробляє та затверджує: 1) положення про Екзаменаційну комісію (ЕК); 2) порядок перевірки кваліфікаційних дипломних магістерських робіт на плагіат; 3) нормативи унікальності текстів кваліфікаційних дипломних магістерських робіт. Атестація осіб, які здобувають ступінь магістра, здійснюється ЕК, до складу якої можуть включатися представники роботодавців та їх об'єднань. Атестація здійснюється відкрито і публічно. Дипломна робота магістра допускається до захисту перед ЕК за умови, якщо рівень її унікальності (оригінальності) відповідає нормативу, який офіційно затверджений Харківським національним економічним університетом імені Семена Кузнеця. Вимоги до заключної кваліфікаційної роботи: Кваліфікаційна дипломна магістерська робота – це навчально-наукова робота студента, яка виконується на завершальному етапі здобуття кваліфікації магістра з кібербезпеки для встановлення відповідності отриманих здобувачами вищої освіти результатів навчання (компетентностей) вимогам стандартів вищої освіти. Вона є кваліфікаційним документом, на підставі якого ЕК визначає рівень теоретичної підготовки випускника, його готовність до самостійної роботи за фахом і приймає рішення щодо присвоєння відповідної кваліфікації та видачу диплома. Дипломна робота магістра є інструментом закріплення та демонстрації сформованих упродовж навчання загальних та спеціальних компетентностей відповідно профілю обраної освітньо-професійної програми. Для оприлюднення та публічного ознайомлення зі змістом кваліфікаційних робіт, запобігання академічного плагіату дипломні роботи мають бути розміщені на офіційному сайті Харківського національного економічного університету імені Семена Кузнеця.
Вимоги до публічного захисту (демонстрації за наявності)	У процесі публічного захисту кандидат на присвоєння магістерського ступеня повинен показати уміння чітко і упевнено викладати зміст проведених досліджень, аргументовано відповідати на запитання та вести дискусію. Доповідь студента повинна супроводжуватися презентаційними матеріалами та пояснювальною запискою, призначеними для загального перегляду.

	Ухвалення екзаменаційною комісією рішення про присудження ступеня магістра з кібербезпеки та видачу диплома магістра за результатами підсумкової атестації студентів оголошуються після оформлення в установленому порядку протоколів засідань екзаменаційної комісії.
Вимоги до кваліфікаційного екзамену	Кваліфікаційний екзамен має передбачати оцінювання обов'язкових результатів навчання, визначених освітньо- професійною програмою.

VII. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

Визначаються відповідно до Європейських стандартів та рекомендацій щодо забезпечення якості вищої освіти (ESG) та статті 16 Закону України "Про вищу освіту".

Принципи та процедури забезпечення якості освіти	**Принципи забезпечення якості освіти:** • відповідальність за якість вищої освіти, що надається; • забезпечення якості відповідає різноманітності систем вищої освіти, закладів вищої освіти, програм і студентів; • забезпечення якості сприяє розвитку культури якості; • забезпечення якості враховує потреби та очікування студентів, усіх інших стейкхолдерів та суспільства. **Процедурами забезпечення якості освіти є:** • розробка стратегії і політики в сфері якості вищої освіти; • розробка механізму формування, затвердження, моніторингу та періодичного перегляду освітньо-професійних програм; • розробка системи оцінювання знань здобувачів вищої освіти, науково-педагогічних і педагогічних працівників та регулярного оприлюднення результатів таких оцінювань на офіційному веб-сайті ХНЕУ ім. С. Кузнеця, на інформаційних стендах та в будь-який інший спосіб, згідно з розробленими та затвердженими правилами. • організація підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників; • формування необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньо-професійною програмою; • створення та функціонування інформаційних систем для ефективного управління освітнім процесом; • оприлюднення об'єктивної неупередженої інформації про освітньо-професійні програми, ступені вищої освіти та кваліфікації; • розробка політики щодо ефективної системи запобігання та виявлення академічного плагіату у наукових працях здобувачів вищої освіти; • інших процедур і заходів.
Моніторинг та періодичний перегляд освітніх програм	Здійснюється моніторинг і періодичний перегляд програм з метою забезпечення їх відповідності потребам студентів і суспільства. Моніторинг спрямований на безперервне вдосконалення програм. Про будь-які дії, заплановані або вжиті як результат перегляду, слід інформувати всі зацікавлені сторони. Регулярний моніторинг, перегляд і оновлення освітніх програм мають на меті гарантувати відповідний рівень надання освітніх послуг, а також створює сприятливе й ефективне навчальне середовище для здобувачів вищої освіти. Це передбачає оцінювання: • змісту програми в контексті останніх досліджень у сфері кібербезпеки, гарантуючи відповідність програми сучасним вимогам; • потреб суспільства, що змінюються; • навчального навантаження здобувачів вищої освіти, їх досягнень і результатів завершення освітньо-професійної програми; • ефективності процедур оцінювання студентів; • очікувань, потреб і задоволеності здобувачів вищої освіти змістом та

	процесом навчання; • навчального середовища відповідності меті і змісту програми; якості сервісних послуг для здобувачів вищої освіти.
Програми регулярно переглядають і оновлюють, залучаючи до цього процесу здобувачів вищої освіти, роботодавців та інших стейкхолдерів.	
Щорічне оцінювання здобувачів вищої освіти	Оцінювання здобувачів вищої освіти базується на принципах студентоцентрованого навчання та передбачає наступне: • оцінювачі (експерти) ознайомлені з існуючими методами проведення тестування та екзаменування і отримують підтримку для розвитку власних навичок у цій сфері; • критерії та методи оцінювання, а також критерії виставлення оцінок оприлюднюються заздалегідь; • оцінювання здобувачів вищої освіти дозволяє продемонструвати ступінь досягнення ними запланованих результатів навчання; • оцінювання проводиться предметною комісією у складі більше ніж дві особи; • процедури оцінювання здобувачів вищої освіти повинні враховувати пом'якшувальні обставини; • оцінювання здобувачів вищої освіти є послідовним, прозорим та проводиться відповідно до встановлених процедур; • наявність офіційної процедури розгляду апеляцій здобувачів вищої освіти.
Підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників	Система підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників розробляється у відповідності до діючої нормативної бази та будується на наступних принципах: • обов'язковості та періодичності проходження стажування і підвищення кваліфікації; • прозорості процедур організації стажування та підвищення кваліфікації; • моніторингу відповідності змісту програм підвищення кваліфікації задачам професійного діяльності; • обов'язковості впровадження результатів підвищення кваліфікації в наукову та педагогічну діяльність; • оприлюднення результатів стажування та підвищення кваліфікації.
Підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників	Система підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників розробляється у відповідності до діючої нормативної бази та будується на наступних принципах: • обов'язковості та періодичності проходження стажування і підвищення кваліфікації; • прозорості процедур організації стажування та підвищення кваліфікації; • моніторингу відповідності змісту програм підвищення кваліфікації задачам професійного діяльності; • обов'язковості впровадження результатів підвищення кваліфікації в наукову та педагогічну діяльність; • оприлюднення результатів стажування та підвищення кваліфікації.
Наявність необхідних ресурсів для організації освітнього процесу	Вищі навчальні заклади забезпечують освітній процес необхідними та доступними для здобувачів вищої освіти ресурсами (кадровими, методичними, матеріальними, інформаційними та ін.) та здійснюють відповідну підтримку студентів. При плануванні, розподілі та наданні навчальних ресурсів і забезпеченні підтримки здобувачів вищої освіти враховуються потреби різноманітного студентського контингенту (такого як студенти: з досвідом, заочної форми навчання, працюючі, іноземні, з особливими потребами) та принципи студентоцентрованого навчання.

	Внутрішнє забезпечення якості освіти гарантує, що всі необхідні ресурси відповідають цілям навчання, є загальнодоступними, а студенти поінформовані про їх наявність.
Наявність інформаційних систем для ефективного управління освітнім процесом	З метою управління освітніми процесами розроблено ефективну політику в сфері інформаційного менеджменту та відповідну інтегровану інформаційну система управління освітнім процесом. Дана система передбачає автоматизацію основних функцій управління освітнім процесом, зокрема: забезпечення проведення вступної кампанії, планування та організація навчального процесу; доступ до навчальних ресурсів; обліку та аналізу успішності здобувачів вищої освіти; адміністрування основних та допоміжних процесів забезпечення освітньої діяльності; моніторинг дотримання стандартів якості; управління знаннями та інноваційний менеджмент; управління кадрами та ін.
Публічність інформації про освітні програми, ступені вищої освіти та кваліфікації	Достовірна, об'єктивна, актуальна, своєчасна та легкодоступна інформація про діяльність за спеціальністю 125 "Кібербезпека" публікується на сайті ХНЕУ ім. С. Кузнеця, включаючи програми для потенційних здобувачів вищої освіти, студентів, випускників, інших стейкхолдерів і громадськості. Надається інформація про освітню діяльність за спеціальністю 125"Кібербезпека", включаючи програми, критерії відбору на навчання; заплановані результати навчання за цими програмами; кваліфікації; процедури навчання, викладання та оцінювання, що використовуються; прохідні бали та навчальні можливості, доступні для студентів тощо.
Запобігання та виявлення академічного плагіату	Система забезпечення дотримання академічної доброчесності учасниками освітнього процесу, сформована в ХНЕУ ім. С. Кузнеця, базується на таких принципах: дотримання загальноприйнятих принципів моралі; демонстрація поваги до Конституції і законів України і дотримання їхніх норм; повага до всіх учасників освітнього процесу незалежно від їхнього світогляду, соціального стану, релігійної та національної приналежності; дотримання норм законодавства про авторське право; посилання на джерела інформації у разі запозичень ідей, тверджень, відомостей; самостійне виконання індивідуальних завдань. У випадку порушення принципів академічної доброчесності відповідні особи притягуються до відповідальності відповідно до законодавства та діючих у ХНЕУ ім. С. Кузнеця положень та норм.

Спеціальні вимоги до зарахування: Набір на спеціальність освітнього рівня "магістр" здійснюється на загальних умовах вступу за результатами фахового випробування:

1) з іноземної мови за результатами незалежного зовнішнього тестування;
2) за комплексом навчальних дисциплін з галузі знань 12 "Інформаційні технології" та з урахуванням середнього балу документа про вищу освіту першого (бакалаврського) рівня.

Для успішного засвоєння освітньо-професійної програми магістра абітурієнти повинні мати перший (бакалаврський) рівень вищої освіти (диплом бакалавра), підтверджений документом державного зразка, що виданий закладом вищої освіти III-IV рівня акредитації.

Профіль програми: інтелектуальні системи і блокчейн технології

Ключові результати навчання за освітньо-професійною програмою "Кібербезпека":
– законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;
– принципів формування систем забезпечення інформаційної та/або кібербезпеки;
– принципів забезпечення безпеки у мережевих пристроях;
– теорії децентралізованих систем управління на основі блокчейн технології;
– методів та засобів виявлення, управління та ідентифікації ризиків;
– методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації;
– методів та засобів технічного та криптографічного захисту інформації.

Професійні профілі випускників: магістр здатний виконувати професійні роботи (за Державним класифікатором професій ДК 003: 2010):
1210.1 Керівники підприємств, установ та організацій;
1229.3 Керівні працівники апарату місцевих органів державної влади;
1236 Керівники підрозділів комп'ютерних послуг;
1238 Керівники проектів та програм;
1495 Менеджери (управителі) систем з інформаційної безпеки;
2132.2 Розробники комп'ютерних програм;
231 Викладачі університетів та вищих навчальних закладів;
2433.1 Наукові співробітники (інформаційна аналітика);
2433.2 Професіонали в галузі інформації та інформаційні аналітики;
2144.1 Наукові співробітники (електроніка, телекомунікації);
2144.2 Інженери в галузі електроніки та телекомунікацій;
2447.1 Наукові співробітники (проекти та програми);
2447.2 Професіонали з управління проектами та програмами.

VIII. Перелік нормативних документів, на яких базується освітньо-професійна програма

Освітня діяльність Харківського національного економічного університету імені Семена Кузнеця ґрунтується на концептуальних засадах Національної Доктрини розвитку освіти, Державній Національній програмі "Освіта" ("Україна XXI століття"), Законі України "Про освіту", Законі України "Про вищу освіту", наказах Міністерства освіти і науки, Статуті Харківського національного економічного університету ім. С. Кузнеця, Тимчасовому Положенні "Про організацію освітнього процесу в Харківському національному економічному університеті імені Семена Кузнеця", затвердженому Вченою радою університету 21.12.2015 року протокол № 6, Тимчасовому Положенні "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговую системою", затвердженому Вченою радою університету 30.08.2013 року протокол № 1, Правилах розпорядку Університету та інших нормативно-правових актах, Тимчасовому положенні "Про освітні програми", затвердженому Вченою радою університету 17.10.2017 року протокол № 2.

Перелік використаних джерел

1. Закон "Про вищу освіту" – http://zakon4.rada.gov.ua/laws/show/1556-18.
2. Національний класифікатор України: "Класифікатор професій" ДК 003:2010.– К. : Видавництво "Соцінформ", 2010. – 746 с.
3. Національна рамка кваліфікацій – http://zakon4.rada.gov.ua/laws/show/1341-2011-п.
4. Перелік галузей знань і спеціальностей – http://zakon4.rada.gov.ua/laws/show/266-2015-п.
5. Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти – file:///D:/Users/Dell/Downloads/BolonskyiProcessNewParadigmHE.pdf.
6. Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд – http://ihed.org.ua/images/biblioteka/Rozvitok_-sisitemi_zabesp_yakosti_VO_UA_2015.pdf.
7. Розроблення освітніх програм: методичні рекомендації – http://ihed.org.ua/images/biblioteka/rozroblennya_osv_program_2014_tempus-office.pdf.
8. 2015 р. Європейська кредитна трансферно-накопичувана система - Довідник користувача (переклад українською мовою) http://erasmusplus.org.ua/erasmus/ka3-pidtrymka-reform/natsionalna-komanda-ekspertiv-here/materiali-here.html

Пояснювальна записка

Матриця відповідності визначених Стандартом компетентностей дескрипторам НРК та матриця відповідності визначених Стандартом результатів навчання та компетентностей представлені в Таблицях 1 і 2.

Таблиця 1

Матриця відповідності визначених компетентностей дескрипторам НРК

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
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 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. Здатність 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.	+	+	+	+

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
КФ 1. Здатність розробляти та впроваджувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	+	+		
КФ 2. Здатність розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах (інформаційних, інформаційно-телекомунікаційних, автоматизованих).	+	+		+
КФ 3. Здатність розробляти й впроваджувати систему менеджменту інформаційної безпеки та/або кібербезпеки організації, формувати стратегію і політики інформаційної безпеки різних рівнів на базі світових й вітчизняних стандартів з урахуванням кращих практик галузі інформаційних технологій та їх безпеки.	+	+		+
КФ 4. Здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, безпеки інформаційних технологій (в т.ч. хмарних технологій та додатків), а також безпеки бізнес/операційних процесів з метою забезпечення функціонування інформаційно-комунікаційних систем згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	+	+	+	+
КФ 5. Здатність розробляти та впроваджувати систему управління інформаційними активами (ресурсами), володіти методами теорії ризик менеджменту та процесних моделей, розробляти моделі загроз й моделі порушника, а також забезпечувати штатне функціонування системи інформаційної безпеки та/або кібербезпеки організації з використанням сучасних технологій.	+	+	+	+

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
КФ 6. Здатність планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів установи, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.		+	+	
КФ 7. Здатність аналізувати причини та наслідки збоїв або відмов функціонування інформаційних систем, що викликані реалізацією різного класу кіберінцидентів, а також розробляти й впроваджувати методи і заходи відновлення штатного функціонування інфраструктури організації в цілому.		+	+	
КФ 8. Здатність розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, а також систему аудиту і контролю функціонування інформаційно-комунікаційних систем та технологій (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	+	+	+	+
КФ 9. Здатність розробляти та впроваджувати методи і заходи протидії кіберінцидентам, а також здійснювати процедури управління, контролю та розслідування, надавати рекомендації щодо попередження та аналізу кіберінцидентів.	+	+		
КФ 10. Здатність розробляти, впроваджувати, та супроводжувати бізнес/операційні процеси з використанням методів та засобів криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	+	+		
КФ 11. Здатність розробляти, впроваджувати і супроводжувати системи аудиту та моніторингу якості бізнес/операційних процесів інформаційно-комунікаційних систем та технологій, а також системи менеджменту інформаційної безпеки та/або кібербезпеки організації в цілому.	+	+		

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
КФ 12. Здатність проводити науково-освітню діяльність, розробляти та впроваджувати систему управління персоналом, а також проводити та планувати навчання працівників і наукові дослідження в сфері безпеки інформаційно-комунікаційних систем і технологій у відповідність вітчизняним та світовим стандартам галузі інформаційної безпеки та/або кібербезпеки.	+	+	+	+

Таблиця 2

Матриця відповідності визначених Стандартом результатів навчання та компетентностей

Програмні результати навчання	Компетентності																			
	Інтегральна	Загальні							Спеціальні (фахові)											
		КЗ-1	КЗ-2	КЗ-3	КЗ- 4	КЗ-5	КЗ-6	КЗ- 7	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9	КФ-10	КФ-11	КФ-12
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації	+	+	+	+	+	+	+	+					+					+		+
ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність	+					+	+	+		+	+	+	+	+	+	+	+			+
ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат	+									+	+		+	+		+				+

Програмні результати навчання	Компетентності																			
	Інтегральна	Загальні							Спеціальні (фахові)											
		КЗ-1	КЗ-2	КЗ-3	КЗ- 4	КЗ-5	КЗ-6	КЗ- 7	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9	КФ-10	КФ-11	КФ-12
ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності	+	+			+				+	+										+
ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки	+		+		+	+							+	+						+
ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому	+	+	+			+				+										+

Програмні результати навчання	Компетентності																			
	Інтегральна	Загальні							Спеціальні (фахові)											
		КЗ-1	КЗ-2	КЗ-3	КЗ- 4	КЗ-5	КЗ-6	КЗ- 7	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9	КФ-10	КФ-11	КФ-12
ПРН-7 – виявляти, описувати та використовувати систему аналізу зв’язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства)	+	+	+			+					+	+	+							
ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо)	+	+	+			+						+			+	+	+	+	+	+

Програмні результати навчання	Компетентності																			
	Інтегральна	Загальні							Спеціальні (фахові)											
		КЗ-1	КЗ-2	КЗ-3	КЗ- 4	КЗ-5	КЗ-6	КЗ- 7	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9	КФ-10	КФ-11	КФ-12
ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки	+	+	+			+				+								+		+
ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо)	+					+					+				+					+

Програмні результати навчання	Компетентності																			
	Інтегральна	Загальні							Спеціальні (фахові)											
		КЗ-1	КЗ-2	КЗ-3	КЗ- 4	КЗ-5	КЗ-6	КЗ- 7	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9	КФ-10	КФ-11	КФ-12
ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства)	+					+								+	+			+	+	+
ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки	+					+								+	+			+	+	+

Програмні результати навчання	Компетентності																			
	Інтегральна	Загальні							Спеціальні (фахові)											
		КЗ-1	КЗ-2	КЗ-3	КЗ- 4	КЗ-5	КЗ-6	КЗ- 7	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9	КФ-10	КФ-11	КФ-12
ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки	+					+					+	+	+	+		+			+	+
ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії	+	+	+			+				+			+	+					+	+

Програмні результати навчання	Компетентності																			
	Інтегральна	Загальні							Спеціальні (фахові)											
		КЗ-1	КЗ-2	КЗ-3	КЗ- 4	КЗ-5	КЗ-6	КЗ- 7	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9	КФ-10	КФ-11	КФ-12
ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки	+	+	+			+				+			+	+					+	+
ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки	+					+				+					+	+				+

Програмні результати навчання	Компетентності																			
	Інтегральна	Загальні							Спеціальні (фахові)											
		КЗ-1	КЗ-2	КЗ-3	КЗ- 4	КЗ-5	КЗ-6	КЗ- 7	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9	КФ-10	КФ-11	КФ-12
ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки	+					+				+					+	+				+
ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства)	+					+			+	+										+
ПРН-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на підприємстві	+	+																+		+

Програмні результати навчання	Компетентності																			
	Інтегральна	Загальні							Спеціальні (фахові)											
		КЗ-1	КЗ-2	КЗ-3	КЗ- 4	КЗ-5	КЗ-6	КЗ- 7	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9	КФ-10	КФ-11	КФ-12
ПРН-20 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні	+			+			+	+												