ПРИВАТНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ»

ПРОЕКТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

РІВЕНЬ ВИЩОЇ ОСВІТИ Другий рівень
(назва рівня вищої освіти)

СТУПІНЬ ВИЩОЇ ОСВІТИ Магістр
(назва ступеня вищої освіти)

ГАЛУЗЬ ЗНАНЬ F Інформаційні технології
(шифр та назва галузі знань)

СПЕЦІАЛЬНІСТЬ F5 Кібербезпека та захист інформації
(код та найменування спеціальності)

Київ - 2025

ЛИСТ ПОГОДЖЕННЯ

ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «КІБЕРБЕЗПЕКА»

ГАЛУЗЬ ЗНАНЬ	F Інформаційні технології
СПЕЦІАЛЬНІСТЬ	F5 Кібербезпека та захист інформації
РІВЕНЬ ВИЩОЇ ОСВІТИ	другий
СТУПІНЬ	магістр

РОЗРОБЛЕНО

Проектною групою
факультету інформаційних систем
та технологій
Гарант освітньо-професійної програми
_____ В.І. Пашорін
«____» _____ 2025 р.

ПОГОДЖЕНО:

Проректор з навчально-методичної роботи
_____ С.М. Ягодзінський

Завідувач навчальної частини
_____ А.О. Козинець

ПЕРЕДМОВА

Проект освітньо-професійної програми викладено на громадське обговорення. Пропозиції, рекомендації та зауваження до змісту ОПП просимо стейкхолдерів надсилати до 25.03.2025 р. за адресою - techno.kafedra@e-u.edu.ua

Освітньо-професійна програма розроблена проектною групою факультету інформаційних систем та технологій у складі:

Пашорін Валерій Іванович - кандидат технічних наук, професор, завідувач кафедри кібербезпеки та захисту інформації;

Яровий Роман Олександрович - кандидат технічних наук, декан факультету інформаційних систем та технологій;

Ніколаєвський Олександр Юрійович - кандидат технічних наук, доцент;

Освітньо-професійна програма розроблена спільно з стейкхолдерами - Міжнародним інноваційним EdTech центром **DAN.IT Education, ТОВ "Консалтингова компанія "СІДКОН", ГО "Асоціація спеціалістів кібербезпеки".**

Освітньо-професійна програма спеціальності F5 "Кібербезпека та захист інформації" розроблена відповідно до стандарту вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації», затвердженого стандарту вищої освіти України: другий (магістерський) рівень, галузь знань 12 Інформаційні технології, спеціальність 125 Кібербезпека та захист інформації. затвердженого і введено в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332. Стандарт розроблено членами підкомісії зі спеціальності 125 Кібербезпека та захист інформації Науково-методичної комісії № 7 з інформаційних технологій, автоматизації та телекомунікацій сектору вищої освіти Науково-методичної ради Міністерства освіти і науки України. Освітня програма для підготовки здобувачів вищої освіти на першому (бакалаврському) рівні за спеціальністю F5 "Кібербезпека та захист інформації" містить обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти; перелік компетентностей випускника; нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання; форм атестації здобувачів вищої освіти; вимоги до наявності системи внутрішнього забезпечення якості вищої освіти; перелік нормативних документів на яких базується освітня програма.

Освітньо-професійна програма затверджена на засіданні кафедри кібербезпеки та захисту інформації ПВНЗ «Європейський університет».

Протокол №

Завідувач кафедри _____ В.І. Пашорін

Профіль
освітньо-професійної програми «Кібербезпека»
зі спеціальності F5 "Кібербезпека та захист інформації"
галузі знань F Інформаційні технології

1. Загальна характеристика	
Повна назва вищого навчального закладу та структурного підрозділу	Приватний вищий навчальний заклад «Європейський університет» Кафедра кібербезпеки та захисту інформації
Ступінь вищої освіти	Другий рівень
Освітня кваліфікація	Магістр з кібербезпеки
Кваліфікація в дипломі	Ступінь вищої освіти – Магістр Спеціальність – F5 Кібербезпека та захист інформації Освітня програма - Кібербезпека
Офіційна назва освітньої програми	Освітньо-професійна програма другого рівня вищої освіти «Кібербезпека»
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний ступінь, 90 кредитів ЄКТС.
Наявність акредитації	Сертифікат про акредитацію з галузі знань (спеціальності) 12 Інформаційні технології 125 Кібербезпека Серія УП №11008523 затверджений рішенням Акредитаційної комісії від 19 лютого 2019 р., протокол №134, наказ МОН України від 25.02.2019 №242 дійсний до 1 липня 2024 року
Цикл/рівень	НРК України – 7 рівень, FQ-ENEA – другий цикл, EQF LLL – 7 рівень

Передумови	Наявність ступеня бакалавра.
Мова навчання	Українська
Термін дії освітньої програми	1 рік 5 місяців
Інтернет - адреса постійного розміщення ОП	https://e-u.edu.ua/ua/pro-universitet/zagalna-informatsija-pro-universitet/osvitni-programi-hidden-block/magistr-info/

2. Мета освітньої програми

Метою магістерської програми "Кібербезпека" є підготовка висококваліфікованих та конкурентоспроможних фахівців, здатних розв'язувати комплексні професійні завдання, використовувати і впроваджувати новітні системи та технології кібербезпеки, провадити науково-дослідну та інноваційну діяльність в галузі захисту інформації і кібербезпеки.

3. Характеристика освітньої програми

Опис предметної області	**Об'єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою;

	– технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. **Цілі навчання:** Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання**. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньо-професійної програми	Освітньо-професійна орієнтація. Поєднання теоретичної та практичної підготовки у сфері кібербезпеки та захисту інформації. Набуття актуальних компетентностей управління персональним освітньо-професійним розвитком, креативного інноваційного мислення з орієнтацією на виконання реальних проектів та

	стартапів в командній роботі, управління проектами з використанням новітніх досягнень науки і техніки.
Основний фокус програми	Спеціальна освіта в галузі 12 Інформаційні технології / спеціальності 125 Кібербезпека та захист інформації. Підготовка фахівців, здатних вирішувати прикладні практичні завдання інформаційної та/або кібербезпеки, розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. Ключові слова: кіберзахист, інформаційна безпека, управління безпекою, інформаційно-комунікаційні системи та мережі.
Особливості програми	Формування відповідних компетентностей у сфері інформаційної та кібернетичної безпеки, насамперед, кібербезпеки інформаційних технологій та систем, в умовах нестабільності інформаційного середовища на основі принципів інноваційного розвитку та сучасних інформаційних технологій, поєднуючи ґрунтовну фундаментальну підготовку із сучасною практичною професійною підготовкою, використовуючи при цьому весь науково-технічний потенціал університету в цій сфері, у першу чергу, залучення науково-педагогічного персоналу, апаратури та обладнання відповідних науково-дослідних лабораторій, надання науково-технічних послуг та виконання наукових-дослідних робіт у галузі криптографічного та технічного захисту інформації. Частина навчальних дисциплін може викладатися англійською мовою.
4. Придатність випускників до працевлаштування та подальшого навчання	
Академічні права випускників	Можливість продовження навчання на третьому (освітньо-науковому) рівні вищої освіти, НРК України – 8 рівень QF-EHEA – третій цикл EQF-LLL – 8 рівень. Набуття додаткових кваліфікацій в системі післядипломної освіти.
Працевлаш-тування випускників	Назви професій згідно Національного класифікатора України: Класифікатор професій (ДК 003:2010 2010 зі змінами від 25.10.21 наказ №810-21 Мінекономіки України): 1495 - Менеджер (управитель) систем з інформаційної безпеки 2149.2 - Професіонал із організації захисту інформації з обмеженим доступом 2149.2 - Професіонал із організації інформаційної безпеки 2131.2 - Науковий співробітник (обчислювальні системи) 2131.2 - Аналітик комп'ютерних систем 251 – Software and applications developers and analysts 252 – Database and network professionals 351 –Information and communications technology operations and user

	support technicians
5.Викладання та оцінювання	
Викладання та навчання (методи, методики, технології, інструменти та обладнання)	Реалізація освітнього процесу передбачає синергетичне поєднання студентоцентрованого, проблемно-орієнтованого і проєктного викладання із застосування наступних технологій і видів навчальних занять: лекції проблемного характеру; мультимедійні та інтерактивні лекції; лабораторні і практичні заняття із розв'язанням ситуаційних завдань та використанням кейс-методів; ділових ігор, тренінги, презентації, що розвивають комунікативні та лідерські навички й уміння працювати в команді; семінари-дискусії; методи мозкового штурму, прес-формул, дерева рішень, самостійна робота з інформаційними джерелами; аналіз і узагальнення інформації; розробка проєктної та програмної документації, реалізація конкретних проєктів, стартапів і робіт прикладного спрямування. Постійне залучення студентів до участі в творчих проєктах (малих колективних роботах), конкурсах, пітчингах інноваційних проєктів, науково-практичних конференціях. Залучення до проведення занять кваліфікованих фахівців-практиків. Переважно заняття відбуваються в малих групах з предметними дискусіями та практичними випробуваннями. Протягом останнього року навчання виділяється час на підготовку випускної кваліфікаційної роботи, яка презентується та обговорюється за участі викладачів, практиків, студентів. Методи, методики та технології: методи та технології розробки систем захисту інформації; збирання, обробки та інтерпретації результатів досліджень. Інструменти та обладнання: програмно апаратні та інструментальні засоби захисту інформації.
Оцінювання	*Оцінювання результатів навчання* здійснюється за національною шкалою оцінювання та системою ECTS. Форми контролю: поточний (захист індивідуальних завдань, тестування, усне і письмове опитування, оцінювання малих колективних робіт); підсумковий (заліки та екзамени з урахуванням балів поточного контролю), підсумкова атестація (комплексна кваліфікаційна робота за фахом).
6. Програмні компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності	КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Спеціальні (фахові, предметні) компетентності	КФ1. 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. КФ2. 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. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. КФ4. 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 та вимог. КФ5. 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. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. 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. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'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. КФ9. 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 в цілому. КФ10. 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.
7. Програмні результати навчання	
Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання	РН1. 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 безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. 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 спеціалізованого програмного забезпечення. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН12. 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. РН13. 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. РН14. 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.

	РН15. Зрозуміло 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. РН16. 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. РН17. 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. РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. РН19. 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. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН22. 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, аргументувати висновки. РН23. 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	

Кадрове забезпечення	Науково-педагогічні працівники, що забезпечують освітній процес, мають відповідну освіту та вагомі здобутки у професійній та/або науковій сферах. Реалізацію ОП «Кібербезпека» другого рівня - магістр вищої освіти забезпечують науково-педагогічні працівники, які мають стаж науково-педагогічної діяльності понад 3 роки та рівень наукової та професійної активності, який засвідчується виконанням не менше чотирьох видів та результатів (підпункти 1-20 пункту 38 Ліцензійних умов провадження освітньої діяльності). Науково-педагогічні працівники регулярно підвищують кваліфікацію у закладах вищої освіти, а також мають сертифікати про проходження теоретичних та прикладних курсів, розробленими відомими компаніями (CISCO, Epam) та навчальними закладами (Stanford University, DeepLearning.AI, Python University, OpenEDG). Окрім науковців теоретичної спрямованості також залучаються фахівці-практики із досвідом роботи 5 років і більше.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення професійної підготовки бакалаврів за ОП відповідає ліцензійним умовам. Загальна площа приміщень університету відповідає ліцензійним вимогам. Площі усіх приміщень відповідають державним будівельним нормам ДБН В 2.2-3-97 «Будинки та споруди навчальних закладів», мають документи про відповідність санітарним нормам та правилам пожежної безпеки. Наявна вся необхідна соціально-побутова інфраструктура, кількість місць в гуртожитках відповідає вимогам. Належним чином обладнані спеціалізовані кабінети, зокрема, навчальні мультимедійні аудиторії з достатньою кількістю комп'ютерних робочих місць. Є доступ до безлімітного користування Інтернет мережею. Комп'ютерні класи оснащені необхідним програмним забезпеченням, зокрема: Linux, Libre Office. Створено університетський Google Workspace. Важливим елементом у підготовці є залучення курсів англійською та українською мовами від навчальних сервісів, зокрема, CISCO Skills for All, Coursera, Epam. Для студентів відкритий безкоштовний доступ з можливістю отримання сертифікатів.
Інформаційне та навчально-методичне забезпечення	Офіційний веб-сайт Університету https://e-u.edu.ua/ua/ містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Всі зареєстровані користувачі мають необмежений доступ до мережі Інтернет. В університеті функціонує бібліотека. Читальний зал

	університету забезпечений бездротовим доступом до мережі Інтернет, періодичними виданнями для забезпечення потреб кожної спеціальності. Матеріали навчально-методичного забезпечення освітньо-професійної програми розроблені викладачами кафедри кібербезпеки та захисту інформації, систематизовані за освітніми компонентами ОП та містять: програми навчальних дисциплін із завданнями до самостійних та індивідуальних робіт, перелік електронних варіантів навчальної літератури в бібліотеці університету та перелік зовнішніх освітньо-інформаційних платформ для проведення занять за ОП спеціальності F5 “Кібербезпека та захист інформації”.
9. Академічна мобільність	
Національна кредитна мобільність	Національна кредитна мобільність реалізується в рамках міжуніверситетських договорів згідно «Положення про академічну мобільність ПВНЗ «Європейський університет».
Міжнародна кредитна мобільність	Міжнародна академічна мобільність відбувається на основі угод про Співробітництво, підписаної між ПВНЗ «Європейський університет» та партнерами поза межами України.
Навчання іноземних здобувачів вищої освіти	Громадяни інших держав приймаються на навчання за спеціальністю F5 «Кібербезпека та захист інформації» відповідно до Правил прийому до ПВНЗ «Європейський університет». Створені умови для підготовки іноземних здобувачів вищої освіти.

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

2.1. Перелік компонент ОПП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ОК 1	Філософія та методологія наукового пізнання	3	залік
ОК 2	Академічна доброчесність та основи академічного письма	3	залік
ОК 3	Методи комплексного кіберзахисту	3	залік
ОК 4	Ділова іноземна мова	3	залік
ОК 5	Стратегічний менеджмент інформаційної безпеки	3	екзамен
ОК 6	Проектування систем кібербезпеки	3	екзамен
ОК 7	Методи і алгоритми криптографії	3	залік
ОК 8	Нормативно-правова база в галузі інформаційної та кібербезпеки та цифрова криміналістика	3	екзамен
ОК 9	Безпека Інтернет-ресурсів	3	екзамен
ОК 10	Математичні методи дослідження операцій	3	екзамен
ОК 11	Аудит безпеки інформаційних систем, тестування на проникнення	5	екзамен
ОК 12	Науково-дослідна практика	5	залік
ОК 13	Фахова практика	10	залік
А	Випускна кваліфікаційна магістерська робота	15	захист
Загальний обсяг обов'язкових компонент:		65 кредитів ЄКТС	
2. Вибіркові освітні компоненти			
ВОК1	Вибіркові освітні компоненти обираються студентами за власними перевагами з каталогу дисциплін, розміщеного на сайті Європейського університету за посиланням	5	залік

ВОК2	https://e-u.edu.ua/ua/pro-universitet/vnutrishnje-zabezpechennja-jakosti-vischoji-osviti/ Загальний обсяг обраних вибіркових компонент має складати 60 кредитів ЄКТС на весь термін навчання. Порядок та процедура вибору здобувачами вибіркових освітніх компонент представлена у Положенні про вибіркові дисципліни Європейського університету, яке розміщено на офіційному сайті за посиланням https://e-u.edu.ua/userfiles/files/208/polozhennya_pro_vibirkovi_disciplini.pdf	5	залік
ВОК3		5	залік
ВОК4		5	залік
ВОК5		5	залік
Загальний обсяг вибіркових компонент		25 кредитів ЄКТС	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90 кредитів ЄКТС	

2.2 СТРУКТУРНО-ЛОГІЧНА СХЕМА

навчальних дисциплін підготовки магістрів зі спеціальності
F5 “Кібербезпека та захист інформації”, освітньо-професійна програма «Кібербезпека»

Перший курс		**Другий курс**
Семестри		
1	**2**	**3**
1. Обов’язкові освітні компоненти		
Філософія та методологія наукового пізнання	Аудит безпеки інформаційних систем, тестування на проникнення	Науково-дослідна практика
Академічна доброчесність та основи академічного письма	Фахова практика	Випускна кваліфікаційна магістерська робота
Методи комплексного кіберзахисту		
Ділова іноземна мова		
Стратегічний менеджмент інформаційної безпеки		
Проектування систем кібербезпеки		
Методи і алгоритми криптографії		
Нормативно-правова база в галузі інформаційної та кібербезпеки та цифрова криміналістика		
Безпека Інтернет-ресурсів		
Математичні методи дослідження операцій		
2. Вибіркові освітні компоненти		
	ВОК1	ВОК3
	ВОК2	ВОК5
	ВОК4	

3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньо-професійної програми «Кібербезпека» за спеціальністю F5 “Кібербезпека та захист інформації” галузі знань F Інформаційні технології проводиться у формі публічного захисту випускної кваліфікаційної роботи.

Кваліфікаційна робота повинна містити розв’язання практичної проблеми в галузі кібербезпеки та захисту інформації та передбачає перевірку досягнення результатів навчання, інтегральної, загальної та фахових компетентностей, визначених освітньою програмою. У кваліфікаційній роботі не має бути академічного плагіату, фальсифікації та фабрикації.

Кваліфікаційна робота має бути оприлюднена на офіційному сайті закладу вищої освіти або його структурного підрозділу, або у репозитарії закладу вищої освіти.

Атестація випускників освітньо-професійної програми «Кібербезпека» спеціальності F5 “Кібербезпека та захист інформації” галузі знань F Інформаційні технології завершується видачею документу встановленого зразка про присудження йому ступеня магістра із присвоєнням кваліфікації: магістр з кібербезпеки та захисту інформації.

4. Перелік нормативних документів, на яких базується Освітня (освітньо-професійна) програма

1. Закон України «Про вищу освіту» 01.07.2014 №1556-VII - Режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18.
2. Наказ Міністерства освіти і науки України від 18.03.21 р. №332 «Про затвердження стандарту вищої освіти за спеціальністю 125 “Кібербезпека” для другого (магістреського) рівня вищої освіти» [Режим доступу: https://mon.gov.ua/storage/app/media/vyshcha/standarty/2021/03/19/125%20Kiberbezpeka_mahistr_18_03_21_332.docx];
3. Стандарти та рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG) // URL: https://ihed.org.ua/wpcontent/uploads/2018/10/04_2016_ESG_2015.pdf .
4. EQF 2017 (Європейська рамка кваліфікацій) // URL: https://ec.europa.eu/ploteus/sites/eac-eqf/files/en.pdf; https://ec.europa.eu/ploteus/content/descriptors-page.
5. QF EHEA 2018 (Рамка кваліфікацій ЄПВО) // URL: http://www.ehea.info/Upload/document/ministerial_declarations/EHEAParis2018_Communique_AppendixIII_952778.pdf
6. ISCED-F (Міжнародна стандартна класифікація освіти – Галузі, МСКО-Г) 2013 // URL: http://uis.unesco.org/sites/default/files/documents/internationalstandard-classification-of-

education-fields-of-education-and-training-2013-detailedfield-descriptions-2015-en.pdf.
7. TUNING (для ознайомлення зі спеціальними (фаховими) та загальними компетентностями та прикладами стандартів – http://www.unideusto/ org/tuningeu/.
8. Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти – http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3 materialy-natsionalnoi-komandy-ekspertiv-shchodo-zaprovadzhennia-instrumentivbolonskoho-protsesu.html?download=82:bolonskyi-protses-nova-paradyhmavyshchoi-osvity-yu-rashkevych&start=80.
9. Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд – http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3-materialy-natsionalnoi-komandy-ekspertiv-shchodozaprovadzhennia-instrumentiv-bolonskoho-protsesu.html?download=88: rozvytoksystemy-zabezpechennia-iakosti-vyshchoi-osvity-ukrainy&start=80.
10. Розроблення освітніх програм: методичні рекомендації / Авт.: В.М. Захарченко, В.І. Луговий, Ю.М. Рашкевич, Ж.В. Таланова / За ред. В.Г. Кременя. – К. ДП "НВЦ "Пріоритети", 2014. – 120 с. – http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3-materialy-natsionalnoikomandy-ekspertiv-shchodo-zaprovadzhennia-instrumentiv-bolonskohoprotsesu.html?download=84: rozroblennia-osvitnikh-prohram-metodychnirekomendatsii&start=80.
11. Положення про систему забезпечення якості освітньої діяльності та якості вищої освіти в ПВНЗ «Європейський університет», обговореного та схваленого Вченою радою Європейського університету (протокол № 6 від 19 грудня 2018 р.).
12. Положення про екзаменаційну комісію з атестації здобувачів вищої освіти в Європейському університеті», обговореного та схваленого Вченою радою Європейського університету (протокол № 1 від 20 лютого 2015 р.).
13. Положення про внутрішню систему забезпечення якості освітньої діяльності», обговореного та схваленого Вченою радою Європейського університету (протокол № 2 від 31 березня 2016 р.)
14. Положення про систему забезпечення якості освітньої діяльності та якості вищої освіти», обговореного та схваленого Вченою радою (Протокол №6 від 19.12.2018р.), в ПВНЗ «Європейський університет».

5. Пояснювальна записка до освітньої (освітньо-професійної) програми

Освітньо-професійна програма “Кібербезпека” спеціальності F5 “Кібербезпека та захист інформації” визначає вимоги до другого (магістерського) рівня вищої

освіти осіб, які можуть розпочати навчання за цією програмою, кількість кредитів ЄКТС, необхідних для виконання цієї програми, а також очікувані результати навчання та компетентності, якими повинен оволодіти здобувач відповідного ступеня вищої освіти.

Базується на компетентнісному підході і поділяє філософію визначення вимог до фахівця, закладену в основу Болонського процесу та в міжнародному проєкті Європейської комісії «Гармонізація освітніх структур в Європі» (Tuning Educational Structures in Europe, TUNING).

Порядок нумерації в переліку загальних та фахових компетентностей не пов’язаний зі значимістю тієї чи іншої компетентності.

Таблиця 1

Матриця відповідності компонентів освітньої програми програмним компетентностям

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК10	ОК11	ОК12	ОК13
КЗ-1								+					+
КЗ-2		+						+					
КЗ-3	+							+					
КЗ-4								+					+
КЗ-5			+	+									
КФ1					+	+				+			
КФ2							+	+					
КФ3						+		+					
КФ4					+			+					
КФ5					+	+				+	+	+	
КФ6			+		+						+		
КФ7						+		+	+	+			
КФ8			+				+						
КФ9					+	+					+		
КФ10								+				+	

Таблиця 2

Матриця відповідності компонентів освітньої програми програмним результатам навчання

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13
РН01				+	+			+					+
РН02					+	+		+	+				+
РН03			+				+					+	
РН04			+			+	+			+			+
РН05						+		+		+			
РН06			+								+		+
РН07					+			+					
РН08			+			+						+	+
РН09					+						+		
РН10					+						+		
РН11					+						+		+
РН12			+			+		+	+			+	+
РН13			+			+	+					+	+
РН14						+					+		
РН15				+	+			+			+		+
РН16					+			+		+			
РН17	+	+		+				+					+
РН18		+			+								+
РН19			+		+				+				
РН20	+				+	+							
РН21										+		+	
РН22	+		+									+	+
РН23			+		+	+							+