ПРИВАТНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ»

ПРОЕКТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

РІВЕНЬ ВИЩОЇ ОСВІТИ Перший (бакалаврський) рівень
(назва рівня вищої освіти)

СТУПІНЬ ВИЩОЇ ОСВІТИ Бакалавр
(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	перший
СТУПІНЬ	бакалавр

РОЗРОБЛЕНО

Проектною групою
факультету інформаційних систем
та технологій
Гарант освітньо-професійної програми
_____ Р.О. Яровий
«____» _____ 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:

Яровий Роман Олександрович – кандидат технічних наук, декан факультету інформаційних систем та технологій (гарант);
Ніколаєвський Олександр Юрійович - кандидат технічних наук, доцент;
Милашенко Віктор Миколайович - старший викладач кафедри кібербезпеки та захисту інформації.

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 наказом Міністерства освіти і науки України від 04 жовтня 2018 року № 1074 (та змінами від 30 квітня 2020 року №584). Стандарти вищої освіти на першому (бакалаврському) рівні за спеціальністю 125 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	Перший (бакалаврський) рівень
Освітня кваліфікація	Бакалавр з кібербезпеки
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – F5 Кібербезпека та захист інформації Освітня програма - Кібербезпека
Офіційна назва освітньої програми	Освітньо-професійна програма першого (бакалаврського) рівня вищої освіти «Кібербезпека»
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний ступінь: - на базі повної загальної середньої освіти обсяг освітньої програми становить 240 кредитів ЄКТС; - на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») визнається та перезарахується не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста) зі спеціальностей галузі знань F Інформаційні технології та не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста) за іншими спеціальностями; - на основі ступеня «фаховий молодший бакалавр» визнається та перераховується не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти.

Наявність акредитації	Сертифікат про акредитацію з галузі знань (спеціальності) 12 Інформаційні технології 125 Кібербезпека Серія УП №11006151 затверджений рішенням Акредитаційної комісії від 3 квітня 2018 р., протокол №129, наказ МОН України від 06.04.2018 №329 дійсний до 1 липня 2028 року
Цикл/рівень	НРК України – 6 рівень, FQ-ENEA – перший цикл, EQF LLL –6 рівень
Передумови	Наявність повної загальної середньої освіти або ступеня «молодший бакалавр», «фаховий молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст»).
Мова навчання	Українська
Термін дії освітньої програми	3 роки 10 місяців
Інтернет - адреса постійного розміщення ОП	https://e-u.edu.ua/ua/pro-universitet/zagalna-informatsija-pro-universitet/osvitni-programi-hidden-block/bakalavr-info/

2. Мета освітньої програми

Підготовка висококваліфікованих та конкурентоспроможних фахівців зі ступенем вищої освіти бакалавр, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, пов'язаних із забезпеченням цілісного підходу до захисту систем від атак хакерів, вірусів, несанкціонованого доступу до конфіденційних даних тощо у різних сферах професійної діяльності.

3. Характеристика освітньої програми

Опис предметної області	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. Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки.

	Теоретичний зміст предметної області Знання – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – 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; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. Інструменти та обладнання: – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньо-професійної програми	Освітньо-професійна орієнтація. Поєднання теоретичної та практичної підготовки у сфері 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 інформаційною безпекою з використанням новітніх досягнень науки і техніки.
Основний фокус програми	Спрямування на поглиблену практичну підготовку відповідно до сучасних ризиків, викликів та загроз в інформаційному просторі. Ключові слова: захист інформації, кібербезпека, інформаційна безпека, інформаційні системи, інформаційні технології, інформаційно-комунікаційні технології
Особливості програми	Особливістю даної освітньо-професійної програми є формування у здобувачів освіти компетентностей та програмних результатів навчання, шляхом поєднання теоретичної та практичної складових

	програми та з урахуванням вимог національного та міжнародного ринку праці.
4. Придатність випускників до працевлаштування та подальшого навчання	
Академічні права випускників	Можливість навчання за програмою другого циклу FQ-EHEA, 7 рівня EQF-LLL (другий рівень вищої освіти) 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): 3439 Інспектор з організації захисту секретної інформації 3439 Фахівець з режиму секретності 3439 Фахівець із організації захисту інформації з обмеженим доступом 3439 Фахівець із організації інформаційної безпеки Згідно класифікатора http://www.cyberdegrees.org/ можливе працевлаштування випускників: P10 Security Analyst P11 Security Specialist P12 Security Administrator P13 Security Engineer P14 Incident Responder P15 Cryptographer P16 Security Software Developer P17 Security Consultant
5.Викладання та оцінювання	
Викладання та навчання (методи, методики, технології, інструменти та обладнання)	Реалізація освітнього процесу передбачає синергетичне поєднання студентоцентрованого, проблемно-орієнтованого і проєктного навчання із застосуванням наступних технологій і видів навчальних занять: лекції проблемного характеру; мультимедійні та інтерактивні лекції; практичні заняття та самостійні роботи із розв’язанням ситуаційних завдань та використанням кейс-методів; ділових ігор, презентацій, що сприяє якісному засвоєнню навчального матеріалу, розвиває навички розробки програмних продуктів, комунікативні та лідерські навички й уміння працювати в команді.

	При викладанні застосовуються новітні методики, такі як: методи мозкового штурму, прес-формул, дерева рішень, аналіз і узагальнення інформації; розробка проєктної документації, реалізація конкретних проєктів, стартапів і робіт прикладного спрямування. Студенти постійно залучаються до участі в творчих проєктах, конкурсах, пітчингах інноваційних проєктів, науково-практичних конференціях за фахом. До проведення окремих занять запрошуються кваліфіковані фахівці-практики. Методи, методики та технології: методи та технології розробки систем захисту інформації; збирання, обробки та інтерпретації результатів досліджень з кібербезпеки. 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 (Єдиний державний кваліфікаційний іспит).
6. Програмні компетентності	
Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та вирішувати 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 застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

7. Програмні результати навчання	
Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання	ПР1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПР2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПР3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; ПР4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; ПР5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; ПР6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; ПР7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; ПР8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; ПР9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; ПР10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; ПР11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; ПР12. Розробляти моделі загроз та порушника; ПР13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; ПР14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; ПР15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; ПР16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;

	ПР17. Забезпечувати процеси захисту та функціонування інформаційно телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних . архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; ПР18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; ПР19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; ПР20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; ПР21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах; ПР22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; ПР23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; ПР24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних 10 (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); ПР25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; ПР26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; ПР27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; ПР28. Аналізувати та проводити оцінку ефективності та рівня

	захищеності ресурсів різних класів в інформаційних та . інформаційно телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; ПР29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; ПР30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; ПР31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; ПР32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; ПР33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; ПР34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; ПР35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; ПР36. Виявляти небезпечні сигнали технічних засобів; ПР37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; ПР38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; ПР39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; ПР40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю .

	характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; ПР41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; ПР42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; ПР43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; ПР44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; ПР45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; ПР46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; ПР47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; ПР48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; ПР49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; ПР50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); ПР51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; ПР52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; ПР53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. ПР54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого . розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

	ПР55. Знати кодекс професійної етики, розуміти соціальну значимість та культурні аспекти кібербезпеки.
8.Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Науково-педагогічні працівники, які забезпечують освітній процес за ОП, мають відповідну освіту та вагомі здобутки у професійній та науковій сферах. Реалізацію ОП Кібербезпека першого (бакалаврського) рівня вищої освіти забезпечують науково-педагогічні та 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). Всі науково-педагогічні працівники, відповідно до укладених графіків підвищують кваліфікацію у закладах вищої освіти або на фахових курсах онлайн платформ (Coursera, Prometheus, Дія. Цифрова освіта, Edera та інші), або в ІТ компаніях. До викладання за ОП залучаються науковці та фахівці практики.
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. 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. Наявна вся необхідна соціально-побутова інфраструктура, кількість місць в гуртожитках відповідає вимогам.
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			
ОК1	Історія української державності та культури	3	залік
ОК2	Ділова українська мова	3	екзамен
ОК3	Фахова іноземна мова	16	екзамен, заліки
ОК4	Вища математика	4	залік
ОК5	Основи академічної доброчесності	3	залік
ОК6	Вступ до фаху	3	залік
ОК7	Правознавство	4	залік
ОК8	Технології створення стартап проектів та командна робота	5	залік
ОК9	Філософія та критичне мислення	4	екзамен
ОК10	Методи та засоби захисту інформації та даних	5	екзамен
ОК11	Законодавча та нормативно-правова база в галузі інформаційної кібербезпеки	5	залік
ОК12	Теорія та пошук інформації	4	залік
ОК13	Об'єктно-орієнтоване програмування	10	екзамен, залік, курсова робота
ОК14	Адміністрування та захист баз даних	8	екзамен, залік
ОК15	Аналіз та відновлення інформаційно-телекомунікаційних систем	5	екзамен

ОК16	Безпека комп'ютерних мереж	7	екзамен
ОК17	Операційні системи та системне адміністрування	5	екзамен
ОК18	Безпека інформаційних систем	8	залік, екзамен
ОК19	Системне програмування	6	залік
ОК20	Комп'ютерні мережі	4	залік
ОК21	Безпека програм та даних	3	екзамен
ОК22	Дослідження операцій та теорія прийняття рішень	5	залік
ОК23	Методи проектування систем кібербезпеки	4	залік
ОК24	Тестування, якість та супровід програмного забезпечення	4	екзамен
ОК25	Основи алгоритмізації та програмування	8	залік екзамен
ОК26	Управління інформаційною та кібербезпекою	4	екзамен
ОК27	Системи та засоби криптографічного захисту	3	екзамен
ОК28	Комплексні системи захисту інформації	5	екзамен
ОК29	Управління ризиками інформаційної безпеки	4	залік
ОК30	Безпека режимних об'єктів	3	екзамен
ОК31	Виробнича практика	15	залік
А1	Єдиний державний кваліфікаційний іспит	3	екзамен
А2	Випускна кваліфікаційна робота бакалавра	6	захист
Загальний обсяг обов'язкових компонент:		**180 кредитів ЄКТС**	
2. Вибіркові освітні компоненти			
ВОК 1	Вибіркові освітні компоненти обираються студентами за власними перевагами з каталогу дисциплін, розміщеного на сайті Європейського університету за посиланням 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_vibirk	5	залік
ВОК 2		5	залік
ВОК 3		5	залік
ВОК 4		5	залік
ВОК 5		5	залік
ВОК 6		5	залік

ВОК 7	ovi_disciplini.pdf	5	залік
ВОК 8		5	залік
ВОК 9		5	залік
ВОК 10		5	залік
ВОК 11		5	залік
ВОК 12		5	залік
Загальний обсяг вибіркових компонент		**60 кредитів ЄКТС**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240 кредитів ЄКТС**	

2.2 СТРУКТУРНО-ЛОГІЧНА СХЕМА

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

1 курс				2 курс				3 курс				4 курс			
1 сем		2 сем		3 сем		4 сем		5 сем		6 сем		7 сем		8 сем	
ОК 1	Історія української державності та культури	ОК 3	Фахова іноземна мова	ОК 3	Фахова іноземна мова	ОК 3	Фахова іноземна мова	ОК 3	Фахова іноземна мова	ОК 3	Фахова іноземна мова	ОК 24	Тестування, якість та супровід програмного забезпечення	ОК 31	Виробнича практика
ОК 2	Ділова українська мова	ОК 5	Основи академічної доброчесності	ОК 9	Філософія та критичне мислення	ОК 13	Об'єктно-орієнтова не програмування	ОК 13	Об'єктно-орієнтова не програмування	ОК 14	Адміністрування та захист баз даних	ОК 27	Системи та засоби криптографічного захисту	ВОК 12	ВОК 12
ОК 6	Вступ до фаху	ОК 7	Правознавство	ОК 13	Об'єктно-орієнтова не програмування	ОК 18	Безпека інформаційних систем	ОК 18	Безпека інформаційних систем	ОК 22	Дослідження операцій та теорія прийняття рішень	ОК 19	Системне програмування	А1	Єдиний державний кваліфікаційний іспит
ОК 8	Технології створення стартап проектів та командна робота	ОК 10	Методи та засоби захисту інформації та даних	ОК 21	Безпека програм та данних	ОК 20	Комп'ютерні мережі	ОК 14	Адміністрування та захист баз даних	ОК 28	Комплексні системи захисту інформації	ОК 16	Безпека комп'ютерних мереж	А2	Випускна кваліфікаційна робота бакалавра
ОК 12	Теорія та пошук інформації	ОК 11	Законодавча на нормативно-правова база в галузі інформаційної та кібербезпеки	ОК 26	Управління інформаційною та кібербезпекою	ОК 23	Методи проектування систем кібербезпеки	ОК 15	Аналіз та відновлення інформаційно-телекомунікаційних систем	ОК 29	Управління ризиками інформаційної безпеки	ВОК 10	ВОК 10		
ОК 25	Основи алгоритмізації та програмування	ОК 17	Операційні системи та системне адміністрування	ОК 30	Безпека режимних об'єктів	ВОК 3	ВОК 3	ВОК 5	ВОК 5	ВОК 8	ВОК 8	ВОК 11	ВОК 11		
ОК 3	Фахова іноземна мова	ОК 25	Основи алгоритмізації та програмування	ВОК1	ВОК 1	ВОК 4	ВОК 4	ВОК 6	ВОК 6	ВОК 9	ВОК 9				
ОК 4	Вища математика			ВОК 2	ВОК 2			ВОК 7	ВОК 7						

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 складання Єдиного державного кваліфікаційного іспиту (ЄДКІ) та захисту випускної кваліфікаційної бакалаврської роботи.

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою.

Кваліфікаційна робота передбачає розв'язок спеціалізованого завдання теоретичного та практичного спрямування в галузі кібербезпеки та захисту інформації. У кваліфікаційній роботі не повинно бути академічного плагіату, фальсифікації та фабрикації.

Кваліфікаційна робота має бути оприлюднена (за виключенням робіт, що містять інформацію з обмеженим доступом) 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 бакалавра із присвоєнням кваліфікації: бакалавр 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 04.10.18 р. №1074 «Про затвердження стандарту вищої освіти за спеціальністю 125 "Кібербезпека" для першого (бакалаврського) рівня вищої освіти» [Режим доступу: https://mon.gov.ua/storage/app/media/vishcha-osvita/2022/Standarty.Vyshchoyi.Osvity/Zatverdzheni.Standarty/01/31/125-Kiberbezpeka-bak.31.01.22.pdf];
3. «Доктрина інформаційної безпеки України», затверджено Указом Президента України від 25 лютого 2017 року № 47/2017.
4. Постанова Кабінету Міністрів «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.04.2015 р. № 266
5. Рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27.01.2016 р., уведеного в дію Указом Президента України від 15.03.2016 р. № 96.
6. Постанова Кабінету Міністрів «Про затвердження Ліцензійних умов провадження освітньої діяльності» від 30.12.2015 № 1187 Наказ МОН України №166 «Деякі питання оприлюднення інформації про діяльність вищих навчальних закладів» від

19.02.2015 р.
7. Наказ МОН України «Про особливості запровадження переліку галузей знань, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29.04. 2015 р.» № 266 від 06.11.2015 р. №1151.
8. Національний класифікатор України: "Класифікатор професій" ДК 003:2010 // Видавництво "Соцінформ". - К.: 2010
9. Наказ Міністерства економічного розвитку і торгівлі України від «Про затвердження зміни до національного класифікатора України ДК 003:2010» від 18.11. 2014 р. № 1361 (зміна № 2)
10. 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.).
11. 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.).
12. Положення про внутрішню систему забезпечення якості освітньої діяльності», обговореного та схваленого Вченою радою Європейського університету (протокол № 2 від 31 березня 2016 р.)
13. 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 F5 «Кібербезпека та захист інформації» визначає вимоги до першого (бакалаврського) 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, закладено в основу Болонського процесу та в міжнародному проекті 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

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31
ЗК1						+							+																		+
ЗК2						+		+																							+
ЗК3	+	+	+						+																						
ЗК4									+		+		+								+										+
ЗК5												+	+																		
ЗК6	+	+					+		+		+																				
ЗК7	+				+																										
КФ 1						+	+				+																			+	+
КФ 2															+		+		+							+	+	+			+
КФ 3										+				+		+			+						+	+					
КФ 4																										+					
КФ 5														+		+		+		+	+						+	+			
КФ 6													+		+						+	+		+							
КФ 7																							+	+						+	
КФ 8																		+			+									+	
КФ 9																										+				+	+
КФ 10				+																+							+			+	
КФ 11															+									+				+	+		
КФ 12										+				+	+														+		

Таблиця 2

Матриця відповідності компонентів освітньої програми програмним результатам навчання

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31
ПР 01		+	+									+																			+
ПР 02	+			+		+						+		+	+																
ПР 03				+					+			+		+	+						+	+							+		
ПР 04				+											+							+							+		+
ПР 05				+		+		+							+							+									
ПР 06									+			+			+								+								
ПР 07						+					+	+			+											+				+	
ПР 08							+				+															+			+	+	
ПР 09							+				+				+																+
ПР 10												+		+	+	+															
ПР 11												+		+	+	+															
ПР 12															+			+											+		+
ПР 13												+				+		+		+											+
ПР 14										+				+	+			+		+		+		+							
ПР 15														+	+					+											+
ПР 16											+							+		+	+							+			
ПР 17														+	+	+	+			+	+										
ПР 18												+			+			+	+	+	+							+			
ПР 19										+					+						+		+								

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31
ПР 20										+					+			+	+		+				+						
ПР 21																								+		+					
ПР 22														+			+									+					
ПР 23																		+			+					+					
ПР 24														+	+		+				+					+					
ПР 25																	+	+													+
ПР 26																+	+														+
ПР 27															+	+	+														
ПР 28															+											+					+
ПР 29															+			+			+								+		
ПР 30															+	+								+							
ПР 31										+				+	+	+															
ПР 32															+											+					+
ПР 33														+								+							+		
ПР 34															+								+			+					
ПР 35																		+										+			+
ПР 36																	+	+		+											
ПР 37												+			+			+													
ПР 38															+	+	+														
ПР 39																												+		+	+
ПР 40												+														+					+

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31
ПР 41																+	+														+
ПР 42															+											+					+
ПР 43											+															+					+
ПР 44											+															+			+		
ПР 45															+							+							+		
ПР 46														+								+							+		
ПР 47												+															+				+
ПР 48																		+									+				+
ПР 49															+		+							+							
ПР 50															+			+			+										
ПР 51															+			+													+
ПР 52															+		+														+
ПР 53													+		+				+						+						
ПР 54	+					+	+				+																			+	
ПР 55					+	+																									+