МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ПРОЄКТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»

першого (бакалаврського) рівня вищої освіти
за спеціальністю F5 Кібербезпека та захист інформації
галузі знань F Інформаційні технології

Тернопіль - 2026

ПЕРЕДМОВА

Розроблено робочою групою у складі:

1. Василь ЯЦКІВ, доктор технічних наук, професор, завідувач кафедри кібербезпеки ЗУНУ;

2. Михайло КАСЯНЧУК, доктор технічних наук, професор, професор кафедри кібербезпеки ЗУНУ;

3. Ігор ЯКИМЕНКО, кандидат технічних наук, доцент, доцент кафедри кібербезпеки ЗУНУ;

4. Степан ІВАСЬЄВ, кандидат технічних наук, доцент, доцент кафедри кібербезпеки ЗУНУ;

5. Сергій КУЛИНА, доктор філософії з кібербезпеки, доцент кафедри кібербезпеки ЗУНУ;

6. Богдан БАРАННІК, викладач кафедри кібербезпеки, випускник освітньо -професійної програми «Кібербезпека» ЗУНУ;

7. Алессандро ЦАРЬКОВ, здобувач освіти першого (бакалаврського) рівня вищої освіти ОПП Кібербезпека, ЗУНУ.

1. Профіль освітньо-професійної програми зі спеціальності F5 Кібербезпека та захист інформації

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Західноукраїнський національний університет, факультет комп'ютерних інформаційних технологій, кафедра кібербезпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр, бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека»
Форма здобуття вищої освіти	денна
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС (на базі повної загальної середньої освіти), 180 (на базі молодшого бакалавра (молодшого спеціаліста), термін навчання 3 роки 10 місяців
Наявність акредитації	Освітня програма акредитована Національним агентством із забезпечення якості вищої освіти №5562, рішення від 11.07.2023 р. Строк дії сертифіката про акредитацію освітньої програми 31.12.2027 р.
Цикл/рівень	Перший (бакалаврський) рівень / НРК України– 6 рівень, FQ-EHEA – перший цикл, EQF LLL – 6 рівень.
Передумови	Повна загальна середня освіта, освітні ступені: «молодший бакалавр», «молодший спеціаліст».
Мова(и) викладання	Українська
Термін дії освітньої програми	Термін не може перевищувати 3 рік 10 місяців.
Інтернет-адреса постійного розміщення опису освітньої програми	https://www.wunu.edu.ua
2 – Мета освітньої програми	
Підготовка висококваліфікованих, конкурентоспроможних фахівців, здатних розробляти і використовувати технології інформаційної безпеки та/або кібербезпеки; які мають теоретичні знання та сформоване критичне мислення; володіють сучасними криптографічними методами захисту інформації; методами захисту мережевої інфраструктури та Web ресурсів; вміють безконфліктно та продуктивно працювати в командах щодо розв'язання проблем та прийняття рішень з питань захисту інформації, безперебійного функціонування, оперативного реагування та відновлення роботи після несанкціонованого втручання в інформаційні системи.	
3 - Характеристика освітньої програми	
Опис предметної області	**Об'єкти вивчення** Наукові та інженерні основи технологій кібербезпеки та захисту інформації, технології, методи, моделі та засоби інформаційної та кібербезпеки, процеси управління кібербезпекою та захистом інформації, безпека інформаційних ресурсів, систем та технологій, штучного інтелекту, об'єктів інформаційної діяльності та критичної інфраструктури.

	Цілі навчання Підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теорії, поняття, концепції, принципи захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, безпеки інформаційних систем та технологій, забезпечення своєчасного виявлення, запобігання і нейтралізації цільових (змішаних) атак, об’єктів інформаційної діяльності та критичної інфраструктури у кіберпросторі. **Методи, методики та технології:** Методи, методики та технології, дослідження, моделювання, аналізу та вдосконалення процесів створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів, розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації у кіберпросторі, виявлення, аналізу кіберінцидентів і протидії ним, запобігання і нейтралізації реальних і потенційних загроз інформаційним ресурсам, об’єктам інформаційної діяльності та критичної інфраструктури, створення, супроводження та забезпечення ефективного функціонування систем захисту інформації, дослідження та вдосконалення процесів обробки та захисту інформаційних ресурсів. **Інструменти та обладнання** Прикладне та спеціалізоване програмне забезпечення, мережне устаткування, апаратне забезпечення, засоби та пристрої захисту інформації.
Орієнтація освітньої програми	Освітньо-професійна програма з кібербезпеки. Враховуючи різке збільшення кібератак на мережеву інфраструктуру державних та приватних організацій ОПП орієнтується на поглиблене вивчення мережевої безпеки, включаючи тестування на проникнення, а також на захисті Web ресурсів, так як більшість зовнішніх атак на корпоративні інформаційні системи націлені саме на вразливості веб-додатків.
Основний фокус освітньої програми	ОП фокусується на формуванні та розвитку у здобувачів професійних компетентностей (застосовувати методи криптографічного захисту інформації; пошук, оцінювання вразливостей та захист Web-додатків; здійснювати тести на проникнення в комп’ютерні системи та мережі шляхом виявлення та експлуатації наявних вразливостей), поєднання яких створює умови для вирішення складних задач щодо захисту програмного забезпечення, мережевої інфраструктури та Web - ресурсів. Ключові слова: кібернетична безпека, криптографія, безпека комп’ютерних мереж, управління інформаційною безпекою, безпека веб-ресурсів, тестування на проникнення.
Особливості програми	Іноваційність, імплементація курсів мережевої академії Cisco в навчальний процес, практична орієнтованість на вирішення актуальних завдань та проблем у інформаційної та/або кібербезпеки. Високий рівень практичної підготовки фахівців забезпечується розвиненою міжнародною співпрацею в науковій і

	освітній сферах, виконання науково-дослідних проєктів, залученням викладачів практиків, наявністю спеціалізованих лабораторій.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець може займати первинні посади (за ДК 003:2010): 2132.2- Розробник систем захисту інформації; 2139.2- Адміністратор мереж і систем; 2139.2- Фахівець з криптографічного захисту інформації; Фахівець з питань безпеки (інформаційно-комунікаційні технології); Аналітик загроз безпеки. International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT).
Подальше навчання	Бакалавр може продовжувати навчання на другому (магістерському) рівні вищої освіти
5 – Викладання та оцінювання	
Викладання та навчання	Студентсько-центроване навчання, самонавчання, проблемно-орієнтоване навчання, кредитно-трансферна система організації навчання, навчання з використанням системи дистанційного навчання Moodle, викладання курсів мережевої академії Cisco, навчання на основі досліджень, навчання через лабораторну практику, використання онлайн лабораторій: TryHackMe, RootMe, HackTheBox, використанням елементів дуальної освіти, розв'язування прикладних задач, виконання проектів, навчальних та виробничих практик, курсових робіт та кваліфікаційної роботи.
Оцінювання	Модульний контроль, заліки, усні екзамени, тести, поточне опитування, тренінги, міждисциплінарна курсова робота, звіт про проходження практики. Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (ЗК)	ЗКІ. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК 4. Здатність спілкуватися іноземною мовою. ЗК 5. Здатність вчитися і оволодівати сучасними знаннями. ЗК6.Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні. ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК 8. 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	СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.) СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності. СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об’єктах інформаційної діяльності. СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
7 – Результати навчання	
РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків. **РН2.** Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. **РН3.** Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. **РН4.** Організовувати власну професійну діяльність, обирати й використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. **РН5.** Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. **РН6.** Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. **РН7.** Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. **РН8.** Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.	

РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.
РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.
РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.
РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Всі науково-педагогічні працівники, залучені до реалізації освітньо-професійної програми мають науковий ступінь і/або вчене звання та підтверджений рівень наукової і професійної активності, що відповідає вимогам ліцензійних умов. Усі науково-педагогічні працівники мають показники академічної та професійної кваліфікації відповідно до дисципліни, викладання якої вони забезпечують.
Матеріально-технічне забезпечення	Освітній процес здійснюється в спеціально обладнаних аудиторіях і лабораторіях, які відповідають санітарно-технічним нормам і оснащених сучасним навчальним обладнанням, мультимедійною, комп'ютерною технікою та спеціалізованим програмним забезпеченням, з можливістю постійного доступу до мережі Internet та внутрішньої мережі ЗУНУ.

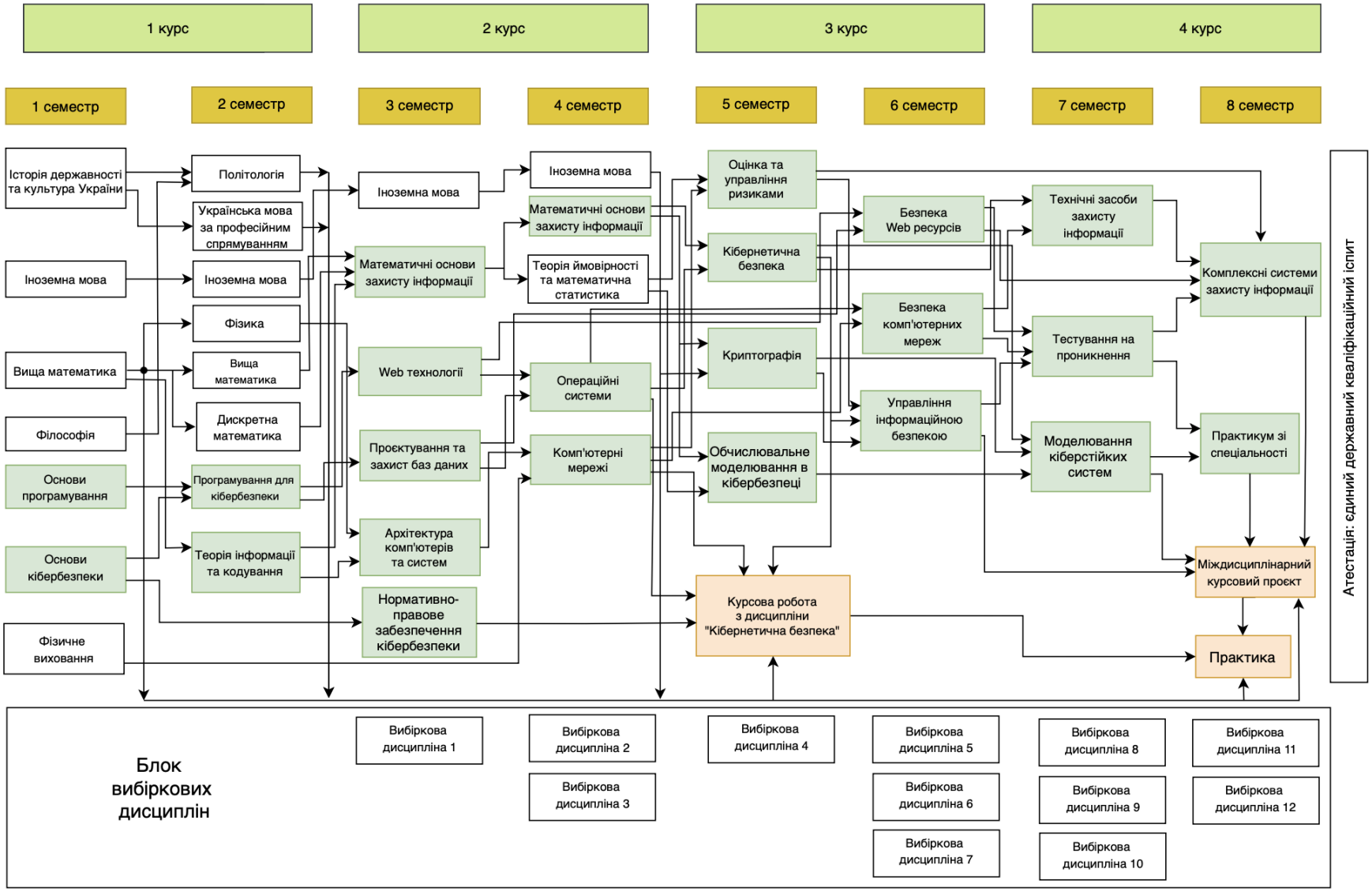
	Комп'ютерна лабораторія обладнана наступним устаткуванням: проектор мультимедійний BenQ TH671ST (1 шт.); комп'ютери на базі процесора Intel Xeon W3550, (10 шт): системний блок Precsion T3500 Westmere. N-serie; монітор Dell E2211H 21.5in.; лабораторні стенди на базі одноплатних комп'ютерів Raspberry Pi – 15 шт.; цифровий осцилограф SIGLENT SDS1202X ; маршрутизатор VPN Router Cisco SB RV320 Dual Gigabit WAN VPN; детектор електромагнітного випромінювання СС308
Інформаційне та навчально-методичне забезпечення	Онлайн-бібліотека, електронні навчально-методичні комплекси дисциплін, робочі програми дисциплін, методичні рекомендації та вказівки до вивчення дисциплін, написання міждисциплінарної курсової роботи, проходження практики і написання випускної кваліфікаційної роботи. Офіційний веб-сайт https://www.wunu.edu.ua/ містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти, тощо. Вільний доступ через сайт ЗУНУ до баз даних періодичних фахових наукових видань (в тому числі, англійською мовою) забезпечується участю бібліотеки університету у консорціуму ElibUkr.
9 – Академічна мобільність	
Національна кредитна мобільність	Відповідно до угод ЗУНУ.
Міжнародна кредитна мобільність	Відповідно до угод ЗУНУ та угод про міжнародну академічну мобільність (Еразмус К1)
Навчання іноземних здобувачів вищої освіти	Відповідно до нормативно-правових документів.

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

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ (ОК)			
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
ОК 1	Історія державності та культура України	4	екзамен
ОК 2	Українська мова за професійним спрямуванням	3	залік
ОК 3	Фізичне виховання	2	залік
ОК 4	Іноземна мова	7	залік, екзамен
ОК 5	Філософія	4	екзамен
ОК 6	Політологія	3	залік
ОК 7	Вища математика	9	залік, екзамен
ОК 8	Теорія ймовірності та математична статистика	4	екзамен
ОК 9	Фізика	4	екзамен
Разом		40	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОК 10	Основи програмування	5	екзамен
ОК 11	Основи кібербезпеки	8	екзамен
ОК 12	Дискретна математика	5	екзамен
ОК 13	Програмування для кібербезпеки	5	екзамен
ОК 14	Теорія інформації та кодування	4	екзамен
ОК 15	Web технології	5	екзамен
ОК 16	Проектування та захист баз даних	5	екзамен
ОК 17	Архітектура комп'ютерів та систем	5	екзамен
ОК 18	Нормативно-правове забезпечення кібербезпеки	5	екзамен
ОК 19	Математичні основи захисту інформації	9	залік, екзамен
ОК 20	Операційні системи	5	екзамен
ОК 21	Комп'ютерні мережі	6	екзамен
ОК 22	Обчислювальне моделювання в кібербезпеці	5	екзамен
ОК 23	Оцінка та управління ризиками	5	екзамен
ОК 24	Кібернетична безпека	6	екзамен
ОК 25	Криптографія	6	екзамен
ОК 26	Безпека комп'ютерних мереж	6	екзамен
ОК 27	Безпека Web ресурсів	5	екзамен
ОК 28	Управління інформаційною безпекою	4	екзамен
ОК 29	Технічні засоби захисту інформації	4	екзамен
ОК 30	Тестування на проникнення	5	екзамен
ОК 31	Моделювання кіберстійких систем	4	екзамен
ОК 32	Комплексні системи захисту інформації	4	екзамен
ОК 33	Практикум зі спеціальності	4	екзамен
ОК 34	Курсова робота з дисципліни "Кібернетична безпека"	3	захист
ОК 35	Міждисциплінарний курсовий проєкт	3	захист
ОК 36	Практика	9	захист
	Єдиний державний кваліфікаційний іспит		екзамен
Разом		140	
Разом обсяг обов'язкових компонент		180	
ВИБІРКОВІ КОМПОНЕНТИ		60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

2.1. Структурно-логічна схема ОПП «Кібербезпека»



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	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	ОК32	ОК33	ОК34	ОК35	ОК36
ЗК1	+		+							+	+		+			+							+	+								+	+	+	+
ЗК2	+						+	+	+		+	+					+	+	+					+											
ЗК3		+																																		
ЗК4				+																																
ЗК5		+		+	+		+	+	+	+		+																					+	+	+	
ЗК6	+				+	+												+																		
ЗК7						+												+																		
ЗК8	+		+		+	+																														
СК1																		+										+				+				
СК2							+	+	+	+	+	+	+	+	+	+	+		+	+	+	+		+	+	+	+	+	+	+		+				
СК3											+					+						+	+	+		+	+	+			+					+
СК4										+	+		+	+	+				+	+	+			+	+	+	+	+		+		+				
СК5											+											+	+	+		+	+	+		+	+	+				+
СК6																								+				+			+	+				
СК7																								+				+				+				+
СК8																									+											
СК9																													+							
СК10										+			+	+	+					+	+		+			+				+		+				

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

	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	ОК32	ОК33	ОК34	ОК35	ОК36
ПРН1	+	+		+																																
ПРН2				+																																
ПРН3					+	+																														
ПРН4							+	+	+	+	+	+	+																			+	+	+	+	+
ПРН5							+	+	+	+	+	+	+																				+	+	+	
ПРН6			+					+	+	+	+	+																								
ПРН7							+	+	+			+	+	+					+						+											
ПРН8							+	+	+			+	+																								
ПРН9																	+	+																		
ПРН10							+	+		+	+	+	+		+					+	+	+															
ПРН11																						+	+	+					+								
ПРН12										+						+								+		+	+										
ПРН13																+				+	+									+		+	+		+	+
ПРН14																+													+							
ПРН15																										+										
ПРН16																															+					
ПРН17																						+	+	+												
ПРН18																			+						+											
ПРН19																									+											
ПРН20																													+							
ПРН21																												+		+						