

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ**

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ**

першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека та захист інформації

галузі знань 12 Інформаційні технології

Освітня кваліфікація: Бакалавр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО

Вченою радою ВНУ імені Лесі Українки

(протокол №7 від 25 травня 2023 р.)

Освітньо-професійна програма вводиться в дію з
01 вересня 2023 р.

Наказ № 211-з від 25 травня 2023 р.

ПЕРЕЗАТВЕРДЖЕНО

(із внесеними змінами та доповненнями)

Вченою радою ВНУ імені Лесі Українки

протокол № 16 від 25 листопада 2024 р.

Ректор

Анатолій ЦЬОСЬ

Наказ № 444-з від 25 листопада 2024 р.

Луцьк – 2024

ПЕРЕДМОВА

Освітньо-професійна програма є нормативним документом, який регламентує нормативні, компетентнісні, кваліфікаційні, організаційні, навчальні та методичні вимоги до підготовки бакалаврів у галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека та захист інформації**.

Освітньо-професійна програма заснована на компетентнісному підході підготовки фахівця в галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека та захист інформації**.

Освітньо-професійна програма розроблена робочою групою ВНУ імені Лесі Українки у складі:

1. Чернящук Наталія – доктор педагогічних наук, професор кафедри комп'ютерних наук та кібербезпеки
2. Глинчук Людмила – кандидат фізико-математичних наук, доцент кафедри комп'ютерних наук та кібербезпеки
3. Жигаревич Оксана – старший викладач кафедри комп'ютерних наук та кібербезпеки
4. Булатецька Леся – кандидат фізико-математичних наук, доцент кафедри комп'ютерних наук та кібербезпеки
5. Мамчич Тетяна – кандидат фізико-математичних наук, доцент кафедри комп'ютерних наук та кібербезпеки
6. Кухарчук Юрій – оперуповноважений відділу протидії кіберзлочинам у Волинській області Департаменту кіберполіції Національної поліції України, старший лейтенант поліції
7. Геращенко Володимир – CISO в компанії SOC Prime
8. Корольов Богдан – ЗО 4-го року навчання за спеціальністю 125 Кібербезпека та захист інформації
9. Яблонський Володимир – ЗО 4-го року навчання за спеціальністю 125 Кібербезпека та захист інформації

Рецензії та відгуки роботодавців, стейкхолдерів:

1. Мороз Борис – доктор технічних наук, професор, професор кафедри програмного забезпечення комп'ютерних систем Національного технічного університету Дніпровська політехніка
2. Круліковський Борис – кандидат технічних наук, доцент кафедри обчислювальної техніки Національного університету водного господарства та природокористування
3. Мартинюк Ганна – кандидат технічних наук, доцент кафедри системного аналізу та інформаційних технологій Маріупольського державного університету

Освітня програма погоджена вченою радою факультету інформаційних технологій і математики, схвалена науково-методичною комісією факультету інформаційних технологій і математики та затверджена Вченою радою Волинського національного університету імені Лесі Українки.

Порядок розробки, експертизи, затвердження і внесення змін в освітню програму регулюється Порядком формування освітніх програм та навчальних планів підготовки фахівців за першим (бакалаврським) та другим (магістерським) рівнями у Волинському національному університеті імені Лесі Українки та Положенням про розроблення, моніторинг, перегляд та закриття ОП, затвердженими Вченою радою ВНУ імені Лесі Українки.

Ця освітня програма не може бути повністю або частково відтворена, тиражована та розповсюджена без дозволу Волинського національного університету імені Лесі Українки.

1. Профіль освітньо-професійної програми зі спеціальності 125 Кібербезпека та захист інформації

1 – Загальна інформація	
Ступінь вищої освіти	Бакалавр
Освітня кваліфікація	Бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Кібербезпека та захист інформації
Тип диплома та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС
Наявність акредитації	Первинна
Цикл/рівень	НРК України – 6 рівень, FQ-ЕНЕА – перший цикл, EQF-LLL – 6 рівень
Передумови	Повна загальна середня освіта
Форма здобуття освіти	Денна
Мова викладання	Українська мова
Термін дії освітньої програми	3 роки 10 місяців
Інтернет-адреса постійного розміщення опису освітньої програми	https://vnu.edu.ua/uk/all-educations
2 – Мета освітньо-професійної програми	
Освітня програма спрямована на підготовку фахівців, здатних розробляти, впроваджувати та супроводжувати системи захисту в інформаційно-телекомунікаційних системах, вирішувати прикладні завдання проєктування та побудови комплексних систем захисту інформації, а також керування процесами управління інформаційною та кібербезпекою в різного роду загроз.	
3 – Характеристика освітньо-професійної програми	
Предметна область (галузь знань, спеціальність)	12 Інформаційні технології 125 Кібербезпека та захист інформації Об'єкти вивчення: - технології кібербезпеки та захисту інформації; - процеси управління кібербезпекою та захистом інформації; - об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. Теоретичний зміст предметної області: Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час

	використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Методи, методики та технології: методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. Включаючи але не обмежуючись міжнародними стандартами та фреймворками ISO/IEC 27000, NIST SP 800-53, NIST CSF, MITRE ATT&CK, OWASP, тощо. Інструменти та обладнання: засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Орієнтація освітньої програми	Освітньо-професійна програма з кібербезпеки та захисту інформації орієнтована на підготовку фахівців, здатних забезпечувати конфіденційність, цілісність і доступність інформаційних ресурсів. Програма акцентує увагу на вивченні методів захисту інформації, виявленні та нейтралізації кіберзагроз, а також запобіганні витоку даних. Здобувачі набувають знань та практичних навичок для роботи в сфері IT-безпеки, аналізу ризиків, управління інцидентами кібербезпеки та протидії кіберзлочинності.
Основний фокус освітньої програми та спеціалізації	Загальна вища освіта першого (бакалаврського) рівня в галузі інформаційних технологій за спеціальністю Кібербезпека та захист інформації. Акцент програми здійснено на проектуванні, впровадженні, супроводі та оцінці комплексних систем захисту інформації, систем управління інформаційною та/або кібербезпекою в умовах сучасного ландшафту загроз, на розробці політик інформаційної та/або кібербезпеки, на використанні засобів приймання, передавання та обробки сигналів в системах технічного захисту інформації. Програма базується на сучасних підходах до захисту інформації, виявлення та протидії кіберзагрозам. Ключові слова: кібербезпека, інформаційна безпека, комплексні системи захисту, технічні засоби захисту, інформаційно-комунікаційні системи, системи управління інформаційною та/або кібербезпекою.
Особливості програми	Особливість програми полягає у врахуванні регіональних особливостей ринку праці, сформованого, переважно, представниками малого та середнього бізнесу, які зацікавлені у поєднанні компетенцій суміжних IT-спеціальностей в одному фахівці, у застосуванні технологій управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Однією з ключових переваг програми є взаємовигідна колаборація ВНУ імені Лесі Українки з органами місцевого

	самоврядування регіону, регіональними структурами кіберполіції, Держспецзв'язку та Служби безпеки України як суб'єктів забезпечення кібербезпеки України. Впродовж усього навчання практикуючі фахівці з кібербезпеки та захисту інформації відповідних служб залучаються до проведення лекцій та практичних занять. Студенти в свою чергу залучаються до практичної роботи у відповідних органах за спеціальністю. Окремо за підтримки CDTO Волинської Облдержадміністрації (заступник з цифрової трансформації) студенти з програми мають можливість долучатися до подій загальноукраїнського та міжнародного рівня, таких як CTF, конференції, тощо.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть бути працевлаштовані на посади у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності 125 Кібербезпека та захист інформації (першого бакалаврського рівня вищої освіти). Працевлаштування в організаціях та підприємствах будь-якої форми власності на посадах згідно з редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010, чинний, зі змінами, внесеними 16.01.2024, а також згідно http://www.cyberdegrees.org/
Подальше навчання	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття та вдосконалення освіти та професійної підготовки в системі освіти дорослих. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Викладання та навчання ґрунтуються на принципах студентоцентрованого та індивідуально-особистісного підходу. Основними видами навчальних занять є аудиторні заняття (лекція, лабораторне та практичне заняття), консультації, самостійна та індивідуальна робота, практична підготовка (навчальні та виробничі практики), контрольні заходи (екзамен, залік, контрольна робота), курсові роботи. НПП поєднують традиційні та інноваційні методи викладання освітніх компонентів. Навчально-методична та консультативна підтримка освітніх компонентів з елементами дистанційного навчання здійснюється через факультетське та університетське середовище LMS Moodle https://moodle.vnu.edu.ua , https://moodle-cs.vnu.edu.ua .
Оцінювання	Оцінювання навчальних досягнень здійснюється на основі принципів академічної доброчесності згідно з Положенням про поточне та підсумкове оцінювання знань студентів ВНУ імені Лесі Українки, враховує всі види аудиторної та позааудиторної освітньої діяльності і має наступну структуру: поточний контроль (усне та письмове

	опитування, захист лабораторних робіт, виступи на практичних заняттях, комп'ютерне тестування, контрольні роботи), підсумковий контроль (тестування, індивідуальне завдання, залік, екзамен, захист практики, захист курсової роботи). Оцінювання навчальних досягнень здобувачів вищої освіти здійснюється за 100-бальною системою згідно зі шкалою ECTS (A, B, C, D, E, F, FX) та національною шкалою (відмінно, дуже добре, добре, задовільно, незадовільно; зараховано, не зараховано). Атестація здійснюється у формі ЄДКІ. ЄДКІ передбачає оцінювання досягнень результатів навчання визначених стандартом за спеціальністю 125 Кібербезпека та захист інформації за цією освітньою програмою.
6 – Перелік компетентностей випускника	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області та 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. ЗК 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 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. СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК 4. Здатність забезпечувати захист інформації

	інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.) СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК 10. 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

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

РН 3. Застосовувати принципи неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН 5. 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.

РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН 7. 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.

РН 8. 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.

РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

- РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
- РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.
- РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
- РН 13. 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.
- РН 14. 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.
- РН 15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
- РН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
- РН 17. 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.
- РН 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
- РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
- РН 20. 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.
- РН 21. 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	Науково-педагогічні працівники, які залучені до підготовки бакалаврів за освітньою програмою Кібербезпека та захист інформації, відповідають ліцензійним вимогам, мають науковий ступінь та/або вчене звання за відповідною або спорідненою спеціальністю, систематично здійснюють наукову і навчально-методичну діяльність, регулярно проходять стажування (підвищують кваліфікацію), у тому числі й за кордоном; їх базова освіта відповідає профілю освітніх компонент, які вони викладають. До освітнього
-----------------------------	---

	процесу за ОП залучаються викладачі практики.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення освітньо-професійної програми відповідає чинним технологічним вимогам до впровадження освітньої діяльності у сфері вищої освіти, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (чинний) в редакції від 24.03.2021 р. № 365: навчальні корпуси, лекційні аудиторії (окремі з них обладнані мультимедійними проєкторами), аудиторії для практичних занять, комп'ютерні класи, лабораторії (лабораторія інформаційних технологій, спільна лабораторія Internet Devels та ЗВО і Центр кібербезпеки та захисту інформації, спільна лабораторія SOC Prime та ЗВО), спеціалізовані кабінети обладнані відповідно до потреб освітнього процесу, комп'ютерне, мережеве та програмне забезпечення, мультимедійне обладнання, бібліотека, Інклюзивний хаб, бездротовий доступ до інтернету в усіх корпусах університету та бібліотеці, соціально-побутова та спортивно-оздоровча інфраструктура. Корпуси та соціальна інфраструктура ЗВО обладнані пандусами для осіб з особливими освітніми потребами та відповідають правилам протипожежної безпеки, санітарним нормам, функціонують укриття.
Інформаційне та навчально-методичне забезпечення	Наявність офіційного вебсайту Волинського національного університету імені Лесі Українки (https://vnu.edu.ua/uk), сторінок факультету та кафедр (http://surl.li/ufaehs), вебсайту кафедри комп'ютерних наук та кібербезпеки (https://cs.vnu.edu.ua/), на яких розміщена основна інформація про наукову та навчально-методичну діяльність (освітньо-професійні програми, навчальні плани, силабуси з освітніх компонентів тощо). Сайт бібліотеки (http://library.vnu.edu.ua), фонди бібліотеки, інституційний репозитарій (https://evnuir.vnu.edu.ua/), фонд кваліфікаційних робіт, наукова періодика, навчально-методичні розробки НПП, які доступні також і у репозитарії університету. На період навчання здобувачеві безкоштовно надається корпоративний обліковий запис у Microsoft365. Надається безкоштовний доступ до ресурсів платформи онлайн-навчання Coursera в межах проєкту Coursera for Campus (Coursera for Ukraine). Існує кілька локальних комп'ютерних мереж і точок бездротового доступу до мережі Інтернет у ЗВО. Дистанційні курси освітніх компонентів розміщено на платформах Moodle https://moodle.vnu.edu.ua , https://moodle-cs.vnu.edu.ua . Мережа факультету є підмережею мережі ЗВО та забезпечує кожен комп'ютер виходом в інтернет через сервер-шлюз. VPN-сервер дозволяє віддалено працювати з ресурсами підмережі. На серверах кафедри розгорнуто файл-сервер, сайт кафедри, Moodle, Open Journal Systems та експериментальний хостинг для здобувачів освіти. Ресурси на цих серверах мають університетські доменні імена (https://cs.vnu.edu.ua , вкладка Наші ресурси). Функціонують

	точки доступу WI-FI в кожній із лабораторій.
9 – Академічна мобільність	
Національна кредитна мобільність	Регламентується Постановою КМУ «Про затвердження Положення про порядок реалізації права на академічну мобільність» №579 від 12.08.2015 р. та Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу Волинського національного університету імені Лесі Українки. На основі двосторонніх договорів між Волинським національним університетом імені Лесі Українки та ЗВО України.
Міжнародна кредитна мобільність	Регламентується Постановою КМУ №579 «Про затвердження Положення про порядок реалізації права на академічну мобільність» від 12.08.2015 р. У рамках програми ЄС Еразмус+ на основі двосторонніх договорів між Волинським національним університетом імені Лесі Українки та закладами вищої освіти країн-партнерів.
Навчання іноземних здобувачів вищої освіти	Передбачена можливість навчання іноземних здобувачів вищої освіти на акредитованих ОП/спеціальностях Волинського національного університету імені Лесі Українки у межах ліцензованих обсягів після вивчення курсу української мови на підготовчому відділенні ННІНО Волинського національного університету імені Лесі Українки.

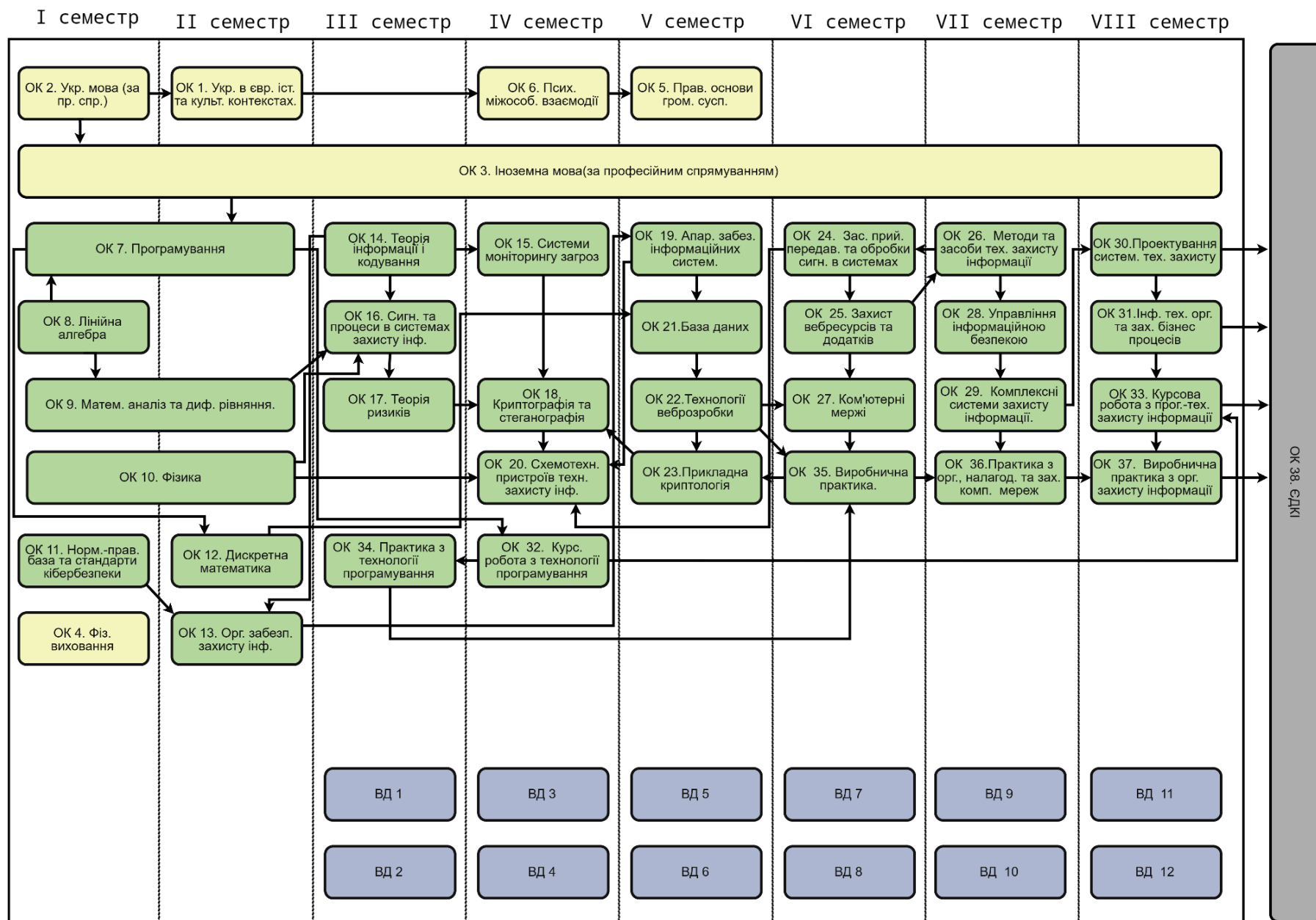
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонент ОП

Код	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти освітньо-професійної програми			
1. Цикл загальної підготовки			
ОК 1.	Україна в європейському історичному та культурному контекстах	3	залік
ОК 2	Українська мова (за професійним спрямуванням)	3	екзамен
ОК 3	Іноземна мова	12	екзамен, залік
ОК 4.	Фізичне виховання	2	залік
ОК 5	Правові основи громадянського суспільства	3	залік
ОК 6.	Психологія міжособистісної взаємодії	3	залік
Разом		26	
2. Цикл професійної підготовки			
ОК 7	Програмування	13	екзамен
ОК 8	Лінійна алгебра	4	екзамен
ОК 9	Математичний аналіз та диференціальні рівняння	10	екзамен, залік
ОК 10	Фізика	10	екзамен, залік
ОК 11	Нормативно-правова база кібербезпеки	4	залік
ОК 12	Дискретна математика	4	екзамен
ОК 13	Організаційне забезпечення захисту інформації	4	залік
ОК 14	Теорія інформації і кодування	5	екзамен
ОК 15	Системи моніторингу загроз	4	залік
ОК 16	Сигнали та процеси в системах захисту інформації	4	екзамен
ОК 17	Теорія ризиків	4	екзамен
ОК 18	Криптографія та стеганографія	5	екзамен
ОК 19	Апаратне забезпечення інформаційних систем	4	екзамен
ОК 20	Схемотехніка пристроїв технічного захисту інформації	4	екзамен
ОК 21	Бази даних	4	екзамен
ОК 22	Технології веброзробки	4	екзамен
ОК 23	Прикладна криптологія	4	екзамен
ОК 24	Інформаційні технології організації та захисту бізнес-процесів	4	екзамен
ОК 25	Захист вебресурсів та додатків	4	екзамен
ОК 26	Методи та засоби технічного захисту інформації	4	екзамен
ОК 27	Комп'ютерні мережі	4	екзамен
ОК 28	Управління інформаційною безпекою	4	екзамен

ОК 29	Комплексні системи захисту інформації	5	екзамен
ОК 30	Проектування систем технічного захисту	4	екзамен
ОК 31	Інформаційні технології організації та захисту бізнес процесів	4	екзамен
ОК 32	Курсова робота з технології програмування	2	залік
ОК 33	Курсова робота з програмно-технічного захисту інформації	2	залік
ОК 34	Практика з технології програмування	6	залік
ОК 35	Виробнича практика	6	залік
ОК 36	Практика з організації, налагодження та захисту комп'ютерних мереж	6	залік
ОК 37	Виробнича практика з організації захисту інформації	6	залік
ОК 38	ЄДКІ	2	екзамен
Разом		154	
Загальний обсяг обов'язкових компонент		180	
3.Цикл вибірових дисциплін			
39	Вибірковий освітній компонент 1	5	залік
40	Вибірковий освітній компонент 2	5	залік
41	Вибірковий освітній компонент 3	5	залік
42	Вибірковий освітній компонент 4	5	залік
43	Вибірковий освітній компонент 5	5	залік
44	Вибірковий освітній компонент 6	5	залік
45	Вибірковий освітній компонент 7	5	залік
46	Вибірковий освітній компонент 8	5	залік
47	Вибірковий освітній компонент 9	5	залік
48	Вибірковий освітній компонент 10	5	залік
49	Вибірковий освітній компонент 11	5	залік
50	Вибірковий освітній компонент 12	5	залік
Загальний обсяг вибірових компонент		60	
Загальний обсяг освітньої програми		240	кредитів

2.2. Структурно-логічна схема освітньо-професійної програми



3. Форми атестації здобувачів вищої освіти

Проміжна атестація передбачає такі форми: для циклу загальної підготовки – екзамени і заліки; для циклу професійної підготовки – екзамени, заліки, захист практики та курсових робіт.

Атестація здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації здійснюється у формі єдиного державного кваліфікаційного іспиту (наказ Міністерства освіти і науки України від 13.01.2022 р. № 26) та завершується видачею документа встановленого зразка про присудження їм ступеня бакалавра з освітньою кваліфікацією бакалавр з кібербезпеки та захисту інформації.

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених Стандартом вищої освіти за спеціальністю 125 Кібербезпека та захист інформації для першого (бакалаврського) рівня вищої освіти (наказ МОН України від 29 жовтня 2024 року №1547) та освітньою програмою.

4. Матриця відповідності загальних компетентностей (ЗК) компонентам освітньо-професійної програми

	ЗК 1.	ЗК 2.	ЗК 3.	ЗК 4.	ЗК 5.	ЗК 6.	ЗК 7.	ЗК 8.
ОК 1.	+	+	+		+	+	+	+
ОК 2	+		+		+	+	+	+
ОК 3	+		+	+	+	+	+	
ОК 4.	+		+		+			+
ОК 5	+	+	+		+	+	+	+
ОК 6.	+		+	+	+	+	+	
ОК 7	+	+	+	+	+	+	+	+
ОК 8	+	+	+		+	+	+	+
ОК 9	+	+	+		+			
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	+	+	+		+	+	+	+
ОК 32	+	+	+	+	+	+	+	+
ОК 33	+	+	+	+	+	+	+	+
ОК 34	+	+			+	+	+	+
ОК 35	+	+	+	+	+	+	+	+
ОК 36	+	+	+	+	+	+	+	+
ОК 37	+	+	+	+	+	+	+	+
ОК 38	+	+	+	+	+	+	+	+

5. Матриця відповідності фахових компетентностей (СК) компонентам освітньо-професійної програми

[illegible]

6 . Матриця відповідності програмних результатів навчання (РН) компонентам освітньо-професійної програми

	РН 1	РН 2	РН 3	РН 4	РН 5	РН 6	РН 7	РН 8	РН 9	РН 10	РН 11	РН 12	РН 13	РН 14	РН 15	РН 16	РН 17	РН 18	РН 19	РН 20	РН 21
ОК 1	+		+		+				+												
ОК 2	+		+						+												
ОК 3	+	+	+						+												
ОК 4	+																				
ОК 5	+		+	+	+	+			+							+			+		
ОК 6	+																				
ОК 7	+		+	+			+	+		+											
ОК 8			+	+	+		+	+													
ОК 9	+							+		+											
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	+		+	+			+	+													
ОК 32	+		+	+			+	+													
ОК 33	+	+	+	+	+	+			+	+		+	+		+	+	+				+
ОК 34	+		+	+			+	+													
ОК 35	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 36	+			+	+	+			+	+		+					+			+	+
ОК 37	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 38	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Гарант освітньої програми

Наталія ЧЕРНЯЦУК