МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

ПРОЄКТ

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Львівського національного університету
імені Івана Франка

Голова Вченої ради

_____ Володимир МЕЛЬНИК

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
“КІБЕРБЕЗПЕКА”

першого (бакалаврського) рівня вищої освіти

За спеціальністю **125 Кібербезпека та захист інформації**

Галузі знань **12 Інформаційні технології**

Львів – 2024

Розроблено та оновлено робочою групою спеціальності 125 Кібербезпека та захист інформації у складі:

1. **Венгерський Петро Сергійович** д.фіз.-мат.н., в.о. завідувача кафедри кібербезпеки - гарант освітньої програми
2. **Пелешко Дмитро Дмитрович** д. техн. н., професор, професор кафедри кібербезпеки;
3. **Винокурова Олена Анатоліївна**, д. техн. наук, професор, професор кафедри кібербезпеки.
4. **Трушевський Вадерій Миколайович,** канд. фіз.-мат.н., доцент кафедри кібербезпеки;
5. **Мусійовський Юрій**, координатор Операційного Центру кібербезпеки компанії СофтСерв;

Гарант освітньої програми _____ Петро ВЕНГЕРСЬКИЙ

(підпис) (ініціали, прізвище)

Пропозиції та зауваження надсилати на електронну адресу:
cybersecurity.dep.ami@lnu.edu.ua

Профіль освітньої програми
зі спеціальності 125 Кібербезпека та захист інформації

1 - Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Львівський національний університет імені Івана Франка, факультет прикладної математики та інформатики
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр бакалавр з кібербезпеки
Офіційна назва освітньої програми	Освітньо-професійна програма “Кібербезпека”
Наявність акредитації	_____
Цикл/рівень	НРК України – 6 рівень, *FQ-EHEA – first cycle, EQF LLL – 6 рівень*
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання – 3 роки 10 місяців
Цикл/рівень	
Передумови	Повна загальна середня освіта або ступінь «молодший бакалавр» (освітньо-кваліфікаційний рівень «молодший спеціаліст»)
Мова викладання	Українська
Термін дії освітньої програми	До повного планового оновлення, не перевищуючи періоду акредитації
1нтернет-адреса постйного розміщення опису освітньої програми	https://ami.lnu.edu.ua/admission/specializations
Підготовка висококваліфікованих фахівців, які здатні використовувати і впроваджувати технології кібербезпеки, володіти засобами і методами криптографічного захисту інформації, використовувати моделі та принципи управління доступом до інформаційних ресурсів; забезпечувати необхідний рівень захищеності інформації з використанням сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій.	

3 - Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	12 Інформаційні технології 125 Кібербезпека та захист інформації 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.
0рієнтація освітньої програми	Освітньо-професійна програма підготовки бакалавра з кібербезпеки спеціальності 125 Кібербезпека та захист інформації.

Основний фокус освітньої програми та спеціалізації	Загальна освіта в галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека та захист інформації. Освітня програма сфокусована на підготовку висококваліфікованих фахівців, які здатні володіти спеціалізованими програмними пакетами щодо захисту даних в інформаційних і телекомунікаційних системах. Значна увага приділяється застосуванню криптографії у кібербезпеці, формуючи відповідні професійні навички, затребувані на ринку праці. Ключові слова: кібербезпека, інформаційна безпека, управління інформаційною безпекою, криптографічні та технічні методи захисту інформації, захист персональних даних, захист інформації, захист від несанкціонованого доступу, менеджмент інформаційної безпеки.
Особливості програми	Програма враховує актуальні вимоги щодо зв'язку теоретичних знань та практичної підготовки фахівців спеціальності 125 Кібербезпека та захист інформації. Особливістю ОП є поєднання грунтовної підготовки фахівців зі знаннями в **галузі криптографічного захисту інформації** та **безпеки інформаційних технологій**. Кадрове забезпечення підсилене залученням фахівців ІТ-сфери та участю студентів в реальних **командних проектах**. Залучення студентів до участі у **CTF змаганнях** з комп'ютерної безпеки розвиває у студентів вміння застосовувати отримані теоретичні знання для практичних задач, розвиток у них нестандартного мислення, різні комунікаційні навички, знання документів, стандартів, політик та законів, що регулюють ринок інформаційної безпеки. Використання сучасних підходів до неформальної освіти в рамках ОП: залучення здобувачів освіти до розв'язання реальних науково-практичних кейсів на **щорічних зимових Data Engineering and Security та літніх AI Summer school IT школах,** у яких під керівництвом викладачів і менторів з ІТ-компаній слухачі реалізують інноваційні проєкти в напрямку кібербезпеки. Подальша співпраця націлена на впровадження дуальної освіти та покращення матеріально-технічної бази підготовки фахівців. Студенти програми всесторонньо розвивають «м'які» навички (критичне мислення, креативність, навички комунікації, відповідальність, робота в команді, тайм-менеджмент), проходять виробничі практики в компаніях-партнерах.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Перелік первинних посад, що може займати випускник- бакалавр за Державним класифікатором України «Класифікатор професій» за ДК 003:2010: 2139.2 Фахівець з криптографічного захисту інформації 2139.2 Фахівець з оцінки заходів захисту інформації (кібербезпеки) 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології) 2139.2 Фахівець сфери захисту інформації Фахівець з криптографічного захисту інформації зорієнтований на фахові компетенності та програмні результати професійного стандарту, який розробляється Національним агентством кваліфікацій.
Подальше навчання	Можливість продовжити навчання за освітньою програмою ступеня магістра.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, проблемно-орієнтоване викладання, електронне навчання в системі Moodle, самонавчання, колабоорративне і проектне навчання на основі виконання виробничої практики та кваліфікаційної роботи. Викладання здійснюється у формі мультимедійних та інтерактивних лекцій,

	семінарів, практичних та індивідуальних занять, самостійного навчання. Застосування проектно-орієнтованого методу навчання з поєднанням індивідуальних завдань з дисциплін курсів та прикладне застосування знань при виконанні мініпроектів.
Оцінювання	Оцінювання здійснюється за 100-бальною шкалою ECTS (A, B, C, D, E, FX) та національною шкалою («відмінно», «добре», «задовільно», «незадовільно»); для недиференційованих заліків – за вербальною шкалою («зараховано», «не зараховано»). *Поточний контроль* – усне та письмове опитування, оцінка роботи в малих групах, тестування, захист індивідуальних завдань. *Підсумковий контроль* – екзамени та заліки з урахуванням накопичених балів поточного контролю. *Атестація* – Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту. Підготовка та публічний захист (представлення) кваліфікаційної роботи. Оприлюднення змісту навчальної дисципліни та критеріїв оцінювання здійснюється через силабуси дисциплін, які розміщені на офіційному сайті університету. Здобувачі зобов'язані дотримуватися принципів академічної доброчесності при виконанні модульних контрольних робіт, поточних завдань, індивідуальних завдань з дисципліни.
6 – Програмні компетентності	
Інтегральна компетентність (ІК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	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 реалізовувати 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 України. 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.
Фахові компетентності	КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення

спеціальності (КФ)	професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 2. Здатність до використання інформаційно- комунікацтйних 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, уразливості та дестабілізуючі чинники в інформаційному просторі та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
7- Програмні результати навчання	
Програмні результати навчання (ПРН)	ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; ПРН 4. 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; ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; ПРН 11.Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; ПРН 12. Розробляти моделі загроз та порушника; ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; ПРН 17. 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; ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

	ПРН 21. 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; ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); ПРН 25. 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; ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; ПРН 29. 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; ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної

	безпеки та/або кібербезпеки відповідно до цілей і завдань організації; ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно- 11 телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; ПРН 36. Виявляти небезпечні сигнали технічних засобів; ПРН 37. 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; ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; ПРН 44. 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; ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних

	системах; ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз; ПРН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні;
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Викладання на ОПП забезпечується висококваліфікованим науково-педагогічними працівниками. Понад 80% науково-педагогічних працівників, задіяних до викладання професійно-орієнтованих дисциплін зі спеціальності 125 «Кібербезпека та захист інформації» мають наукові ступені та вчені звання, також більше 15% у викладанні приймають участь працівники IT-фірм з практичним досвідом у цьому напрямі, більше 10% викладачів проходять спеціалізовані курси в мережній Академії CISCO та навчальній платформі RangeForce. З метою підвищення фахового рівня усі науково-педагогічні працівники не менше ніж один раз на п’ять років проходять стажування в закладах вищої освіти та IT підприємствах Львова.
Матеріально-технічного забезпечення	Використання сучасного програмного забезпечення провідних IT компаній у галузі компютерних технологій та інформаційної безпеки а також стандартизованих вітчизняних апаратно-програмних засобів захисту інформації. Забезпеченість навчальними приміщеннями, комп’ютерними робочими місцями, мультимедійним обладнанням відповідає потребам. Для проведення практичних і лабораторних робіт, інформаційного пошуку та обробки результатів наявні спеціалізовані лабораторії факультету з необхідним апаратним та програмним забезпеченням та відкритим доступом до Інтернет-мережі. Існує дві навчально-комп’ютерні лабораторії зі спеціалізованим програмним та апаратним забезпеченням (мережеве обладнання Cisco, Ajax та HUAWEI), а також навчальні платформи професійного спрямування RangeForce та CISCO Networking Academy LNU.
Інформаційне та навчально-методичне	Офіційний сайт ЛНУ ім. Івана Франка https://lnu.edu.ua/, факультету прикладної математики https://ami.lnu.edu.ua/. Навчально-методичне забезпечення: навчальний план, силабуси навчальних дисциплін, навчальні і

забезпечення	робочі плани, використання в освітньому процесі електронних освітніх ресурсів, технологій змішаного або дистанційного навчання, системи електронного навчання Moodle, наукова бібліотека https://www.lnulibrary.lviv.ua/ , читальні зали; пакет MS Office 365; корпоративна пошта. Інформаційна система "Dekanat". Доступ до наукометричних баз даних Scopus, Web of Science.
9 - Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між університетом та іншими вишами України
Міжнародна кредитна мобільність	На основі двосторонніх договорів між університетом та навчальними закладами країн-партнерів в рамках програми Еразмус+.
Навчання іноземних здобувачів вищої освіти	Можливе, після вивчення курсу української мови

2. Перелік компонент освітньо-професійної/наукової програми та її логічна послідовність

2.1 Перелік компонент ОП

Назва навчальної дисципліни		**Загальний обсяг**		**Форма підсумкового контролю**
		Кредити	Години	
1. НОРМАТИВНІ НАВЧАЛЬНІ ДИСЦИПЛІНИ				
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ				
НД 1	Іноземна мова	16	480	заліки, екзамен
НД 2	Історія України	3	90	залік
НД 3	Фізичне виховання	3	90	залік
НД 4	Історія української культури	3	90	залік
НД 5	Українська мова (за професійним спрямуванням)	3	90	залік + екзамен
НД 6	Філософія	3	90	залік
ЦИКЛ ПРОФЕСІЙНОЇ І ПРАКТИЧНОЇ ПІДГОТОВКИ				
НД 7	Основи кібербезпеки	7	210	екзамен
НД 8	Моделі та методи дискретної математики	4	120	екзамен
НД 9	Основи математичного аналізу та застосування	3	90	екзамен
НД 10	Програмування	12	360	екзамени
НД 11	Застосування дискретної математики в криптології	4	120	екзамен
НД 12	Прикладні основи обчислювальної	3	90	екзамен

	геометрії та алгебри			
НД 13	Основи командної роботи і презентації проектів	10	300	залік
НД 14	Навчальна практика та командні проекти	6	180	залік
НД 15	Застосування теорії ймовірностей в кібербезпеці	3	90	екзамен
НД 16	Операційні системи	3	90	екзамен
НД 17	Основи комп'ютерних мереж	3	90	екзамен
НД 17	Захист сервісів та підтримка IT процесів	3	90	екзамен
НД 18	Тестування на проникнення	4	120	екзамен
НД 19	Прикладна статистика	3	90	екзамен
НД 20	Фізичні основи електроніки	4	120	залік
НД 21	Менеджмент інформаційної безпеки	5	150	залік,екзамен
НД 22	Основи криптографії	6	180	екзамен
НД 23	Безпека комп'ютерних мереж	6	180	екзамен
НД 24	Застосування формальних мов,автоматів та кодів	3	90	залік
НД 25	Прикладна криптологія	7	210	екзамен
НД 26	Комплексні системи захисту інформації	6	180	екзамен
НД 27	Технічні засоби захисту інформації	5	150	залік
НД 28	Обробка сигналів в кібербезпеці	4	120	екзамен
НД 29	Застосування систем штучного інтелекту в кібербезпеці	4	120	екзамен
НД 30	Інструменти SecOps 1	4	120	залік
НД 31	Оцінка ризиків в кібербезпеці	4	120	залік
НД 32	Курсова робота	3	90	залік
НД 33	Події, опрацювання та аналіз логів	4	120	екзамен
НД 34	Інструменти SecOps 2	4	120	екзамен
НД 35	Захист в хмарних технологіях та великих даних	3	90	екзамен
НД 36	Безпека життєдіяльності та охорона праці	3	90	залік
НД 37	Виробнича(переддипломна) практика	3	90	залік
НД 38	Кваліфікаційна робота	3	90	екзамен
Єдиний державний кваліфікаційний іспит				атестація
	Всього	**180**	**5400**	
2. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ				
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ				
ВД 1	Блок вибіркових дисциплін загальноуніверситетської підготовки (ДВВС)	12	360	залік
ЦИКЛ ПРОФЕСІЙНОЇ І ПРАКТИЧНОЇ ПІДГОТОВКИ				
ВД 2.1	Управління ризиками	3	90	залік
ВД 2.2	Обробка зображень та мультимедіа			

ВД 2.3	Програмування паралельних обчислень			
ВД 3.1	Комп'ютерна криміналістика	5	150	залік
ВД 3.2	Адміністрування систем захисту інформації			
ВД 3.3	Великі дані(Big data)			
ВД 4.1	Організація та проведення тестування на проникнення	5	150	залік
ВД 4.2	Застосування Python в кібербезпеці			
ВД 4.3	Розподілені інформаційно-аналітичні системи захисту даних			
ВД 5.1	Методи інтелектуального аналізу даних	5	150	залік
ВД 5.2	Бізнес аналітика			
ВД 6.1	Високопродуктивний комп'ютинг	6	180	залік
ВД 6.2	Технічні канали витоку інформації			
ВД 6.3	Веб проектування, розробка та безпека веб додатків			
ВД 7.1	Методи та засоби технічного захисту інформації.	6	180	залік
ВД 7.2	Технології кібератак			
ВД 7.3	Розробка та безпека мобільних застосунків			
ВД 8.1	Криптологічний аналіз	6	180	залік
ВД 8.2	Безпечне програмування (Secure coding)			
ВД 8.3	Основи протидії кіберзлочинності			
ВД 9.1	Цифрова стеганографія	6	180	залік
ВД 9.2	Застосування технологій штучного інтелекту для захисту медіаконтенту			
ВД 9.3	Технічні канали витоку інформації			
ВД 10.1	Робототехнічні системи та їх захист	6	180	залік
ВД 10.2	Розширені інструменти SecOps			
ВД 10.3	Безпека ігрових додатків			
Всього вибіркових навчальних дисциплін		**60**	**1800**	
Всього за час навчання		**240**	**7200**	