ЗАТВЕРДЖЕНО:
Ректор Дніпровського національного університету імені Олеся Гончара
_____ Поляков М.В.
«10» 09 2020 р.

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»

рівень вищої освіти перший (бакалаврський)

спеціальність 125 Кібербезпека

галузь знань 12 Інформаційні технології

Схвалено:
вченою радою Дніпровського національного університету імені Олеся Гончара
від 10.09 2020 р., протокол № 1

Дніпро
2020

ПЕРЕДМОВА

1. Внесено: кафедра радіоелектронної автоматики фізико-технічного факультету Дніпровського національного університету імені Олеся Гончара

2. Затверджено та надано чинності рішенням вченої ради Дніпровського національного університету імені Олеся Гончара:
- від «29» червня 2017 р., пр. № 15 (перша редакція);
- від «26» жовтня 2017 р., пр. № 4 (зміни для набору 2018-2019н.р.);
- від «21» грудня 2017 р., пр. № 6 (редакція №2);
- від «21» лютого 2019 р., пр. № 9 (редакція №3, зміни для набору 2019-2020 н.р.);
- від «10» вересня 2020р., пр.№1 (редакція №4, від набору 2020-2021 н.р.);
- від «30» червня 2022 р., пр. №12 (редакція№4, зміни ОП).

3. Розробники (робоча група):

Клименко Світлана Володимирівна – кандидат технічних наук, доцент, доцент кафедри радіоелектронної автоматики, фізико-технічного факультету ДНУ;

Малайчук Валентин Павлович – доктор технічних наук, професор, завідувач кафедри радіоелектронної автоматики, фізико-технічного факультету ДНУ;

Рожковський Володимир Фаустович – кандидат технічних наук, доцент, доцент кафедри радіоелектронної автоматики, фізико-технічного факультету ДНУ;

Федорович Анна Ігорівна – кандидат технічних наук, доцент кафедри радіоелектронної автоматики, фізико-технічного факультету ДНУ.

4. При розробці враховані вимоги:

1. *Освітнього стандарту спеціальності:*

Стандарт вищої освіти зі спеціальності 125 Кібербезпека **затверджений** наказом Міністерства освіти і науки України від 04.10 2018 р. № 1074, **вводиться в дію** з 2018/2019 навчального року.

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

1. Вчена рада фізико-технічного факультету: протокол №11 від 04.04.2022 р.
Голова вченої ради _____ *Сергій ДАВИДОВ*

2. Рада з якості ДНУ: протокол № 10 від « 23 » 06 2022 р.
Заступник голови РЗЯВО _____ *Дмитро СВИНАРЕНКО*

Рецензії-відгуки стейкхолдерів

1. Роботодавці:
    1. Богун М.О., директор ТОВ «Каньйон Інжинірінг»
    2. Кулик С.В., начальник відділу технічної охорони в м. Дніпро, «Охоронний холдінг»

2. Здобувачі вищої освіти:

1. Пільгун В., 4 курс, здобувач першого (бакалаврського) рівня вищої освіти, 125 Кібербезпека, ОП – Кібербезпека.

2. Васильківський В.М., 4 курс, здобувач першого (бакалаврського) рівня вищої освіти, 125 Кібербезпека, ОП – Кібербезпека

1. Профіль освітньої програми зі спеціальності 125 КІБЕРБЕЗПЕКА

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	**Дніпровський національний університет імені Олеся Гончара** **Факультет** фізико-технічний **Кафедра** радіоелектронної автоматики
Офіційна назва освітньої програми	Освітня програма: Кібербезпека
Офіційна назва освітньої програми (англійською мовою)	Educational program: Cyber Security
Ступінь вищої освіти та освітня кваліфікація мовою оригіналу	Бакалавр Освітня кваліфікація: бакалавр з кібербезпеки
Кваліфікація в дипломі	Ступінь: бакалавр Спеціальність: 125 Кібербезпека Освітня програма: Кібербезпека
Кваліфікація в дипломі (англійською мовою)	Degree: bachelor Specialty: 125 Cyber Security Educational program: Cyber Security
Професійна кваліфікація	не надається
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців;
Наявність акредитації	Міністерство освіти і науки України Сертифікат про акредитацію спеціальності 125 Кібербезпека : серія НД № 0495177 від 19 жовтня 2017 р. Термін дії- до 1 липня 2022р.
Цикл/рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF LLL – 6 рівень
Передумови	повна загальна середня освіта або ступінь молодшого бакалавра (молодшого спеціаліста)
Форми навчання	денна
Мова(и) викладання	Українська мова
Термін дії освітньої програми	На період дії сертифікату з акредитації спеціальності (відповідно наказу МОН України від 30.10.2017 № 1432) або до проходження первинної акредитації освітньої програми
Інтернет-адреса постійного розміщення опису освітньої програми	www.dnu.dp.ua www.fti.dp.ua
2 – Мета освітньої програми	
Освітня програма охоплює широкий спектр компетентностей випускників щодо інтеграції програмних та апаратних засобів виявлення, моніторингу й забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності, з акцентом на реалізацію систем технічного захисту інформації.	

3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація)	**галузь знань** 12 Інформаційні технології, **спеціальність**125 Кібербезпека **Об'єкт(и) вивчення та\або діяльності:** – 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. поняття та принципи теорії автоматичного керування, систем автоматизації та комп'ютерно-інтегрованих технологій. **Методи, методики та технології:** здобувач має оволодіти методами, методиками, інформаційно-комунікаційними технологіями та іншими технологіями 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 освітньої програми	Освітньо-професійна. Інтеграція програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта в галузі 12 «Інформаційні технології», спеціальності 125 «Кібербезпека»

	Освітня програма здобуття вищої освіти в галузі інформаційних технологій спеціальності «Кібербезпека» сфокусована на здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої обґрунтованості, технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації. Ключові слова: інформаційні технології, кібербезпека, автоматизація, система керування, система автоматизації, комп'ютеризовані системи управління, процеси керування, інформаційно-комунікаційні системи, проектування, системи технічного захисту, комп'ютерні мережі, криптографія, шифрування, кодування.
Особливості програми	Програма передбачає обов'язковою умовою проходження навчальної та виробничої практики на передових підприємствах, що експлуатують або розробляють інформаційні технології, системи технічного захисту інформації. Освітня програма в рамках університетських підписаних угод щодо європейської науково-освітньої інтеграції надає змогу майбутнім бакалаврам пройти стажування за кордоном та включає в себе програму академічної мобільності.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть працювати на первинних посадах за професіями, визначеними Національним класифікатором України: Класифікатор професій ДК 003:2010 (із змінами і доповненнями, внесеними наказом Міністерства економіки України від 25 жовтня 2021 року № 810): 2 Професіонали 21 Професіонали в галузі фізичних, математичних та технічних наук 213 Професіонали в галузі обчислень (комп'ютеризації) 2131 Професіонали в галузі обчислювальних систем 2131.2 Адміністратор бази даних 2131.2 Адміністратор даних 2131.2 Адміністратор доступу 2131.2 Аналітик з комп'ютерних комунікацій 2131.2 Аналітик комп'ютерних систем 2131.2 Аналітик операційного та прикладного програмного забезпечення 2131.2 Аналітик програмного забезпечення та мультимедіа 2131 Фахівець з розробки та тестування програмного забезпечення 2433 Професіонали в галузі інформації та інформаційного аналізу 2433.2 Професіонали в галузі інформації та інформаційні аналітики 3 Фахівці 343 Технічні фахівці в галузі управління 3439 Інші технічні фахівці в галузі управління 3439 Інспектор з організації захисту секретної інформації 3439 Фахівець із організації інформаційної безпеки 3439 Фахівець із організації захисту інформації з обмеженим доступом

	3439 Фахівець з режиму секретності International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT). За КВЕД: 34. Інші фахівці для відповідних спеціальностей Здатні працювати на посадах середнього та вищого рівня управлінського персоналу, у проектних відділах та організаціях, в галузевих науково-дослідних установах і інститутах, а також інших державних та приватних організаціях і підприємствах, пов'язаних з проектуванням, виробництвом і реалізацією технічних і програмних засобів систем захисту інформації, технічних та програмних засобів комп'ютерних інформаційно-комунікаційних систем, у вищих та середніх навчальних закладах в якості викладача, на інженерних посадах за отриманою базовою спеціальністю.
Подальше навчання	Можливість продовження освіти за другим (магістерським) рівнем вищої освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, технологія проблемного і диференційованого навчання, технологія інтенсифікації та індивідуалізації навчання, технологія програмованого навчання, інформаційна технологія, технологія розвивального навчання, кредитно-трансферна система організації навчання, електронне навчання в системі Moodle, Office 365, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекції, мультимедійної лекції, інтерактивної лекції, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультації з викладачами.
Оцінювання	- Екзамени, заліки та диференційовані заліки; звіт та захист лабораторних/практичних робіт; звіти з практик; контрольні роботи; розрахунково-графічні роботи.
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 (ЗК)	*Компетентності, визначені стандартом вищої освіти:* ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області та розуміння професії. ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК 5. Здатність до пошуку, оброблення та аналізу інформації. 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 і свобод людини і громадянина в Україні. ЗК 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 (СК\ФК)	*Компетентності, визначені стандартом вищої освіти:* ФК 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. ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. *Компетентності, визначені закладом вищої освіти:* ФК 13. Здатність застосовувати знання з загальної фізики, електротехніки, електроніки і мікропроцесорної техніки, в обсязі, необхідному для розуміння процесів в системах технічного захисту інформації. ФК 14. Здатність провадити аналіз складових похибки за їх суттєвими ознаками, оперувати складовими похибки/ невизначеності у відповідності з моделями вимірювання,

	застосовувати стандартні методи розрахунку при конструюванні модулів, деталей та вузлів пристроїв та засобів технічного захисту інформації та їх обчислювальних компонент і модулів, виконувати технічні операції при випробуванні, повірці, калібруванні та здійснювати технічні заходи із забезпечення метрологічної простежуваності, правильності, повторюваності та відтворюваності результатів вимірювань і випробувань за міжнародними стандартами. ФК 15. Володіти знаннями новітніх технологій у професійній галузі, зокрема, проектування систем технічного захисту інформації, збору даних та їх архівування для формування бази даних параметрів процесу та їх візуалізації за допомогою засобів людино-машинного інтерфейсу.

7 – Програмні результати навчання

Результати навчання, визначені стандартом вищої освіти:

ПРН1. Здатність **застосовувати** знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

ПРН2. Здатність **організовувати** власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПРН3. Здатність **використовувати** результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН4. Здатність **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;

ПРН5. Здатність **адаптуватися** в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

ПРН6. Здатність **критично** осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

ПРН7. Здатність **діяти** на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

ПРН8. Здатність **готувати пропозиції** до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

ПРН9. Здатність **впроваджувати** процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

ПРН10. Здатність **виконувати** аналіз та декомпозицію інформаційно-телекомунікаційних систем;

ПРН11. Здатність **виконувати** аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;

ПРН12. Здатність **розробляти** моделі загроз та порушника;

ПРН13. Здатність **аналізувати** проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;

ПРН14. Здатність **вирішувати** завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

ПРН15. Здатність **використовувати** сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;

ПРН16. Здатність **реалізовувати** комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;

ПРН17. Здатність **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;

ПРН18. Здатність **використовувати** програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

ПРН19. Здатність **застосовувати** теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

ПРН20. Здатність **забезпечувати** функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

ПРН21. Здатність **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;

ПРН22. Здатність **вирішувати** задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

ПРН23. Здатність **реалізовувати** заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

ПРН24. Здатність **вирішувати** задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

ПРН25. Здатність **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;

ПРН26. Здатність **впроваджувати** заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;

ПРН27. Здатність **вирішувати** задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

ПРН28. Здатність **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;

ПРН29. Здатність **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;

ПРН30. Здатність **здійснювати** оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;

ПРН31. Здатність **застосовувати** теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

ПРН32. Здатність **вирішувати** задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

ПРН33. Здатність **вирішувати** задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

ПРН34. Здатність **приймати** участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

ПРН35. Здатність **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;

ПРН36. Здатність **виявляти** небезпечні сигнали технічних засобів;

ПРН37. Здатність **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;

ПРН38. Здатність **інтерпретувати** результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН39. Здатність **проводити** атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;

ПРН40. Здатність **інтерпретувати** результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН41. Здатність **забезпечувати** неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

ПРН42. Здатність **впроваджувати** процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;

ПРН43. Здатність **застосовувати** національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;

ПРН44. Здатність **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;

ПРН45. Здатність **застосовувати** ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

ПРН46. Здатність **здійснювати** аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;

ПРН47. Здатність **вирішувати** задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;

ПРН48. Здатність **виконувати** впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;

ПРН49. Здатність **забезпечувати** належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;

ПРН50. Здатність **забезпечувати** функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);

ПРН51. Здатність **підтримувати** працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;

ПРН52. Здатність **використовувати** інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;

ПРН53. Здатність **вирішувати** задачі аналізу програмного коду на наявність можливих загроз.

ПРН54. Здатність **усвідомлювати** цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	
Програмні результати, визначені закладом вищої освіти:	
ПР55. Здатність **використовувати** основи фізики, електротехніки, електроніки та схемотехніки і мікропроцесорної техніки на рівні, необхідному для розв'язання типових задач і проблем кібербезпеки ПР56. Здатність **використовувати** теорію ймовірностей та математичну статистику, теорію випадкових процесів в обсязі, необхідному для користування математичним апаратом та методами у професійній галузі. ПР57. Вміти **використовувати** різноманітне спеціалізоване програмне забезпечення для реалізації типових інженерних задач у галузі автоматизації, зокрема, математичного моделювання, автоматизованого проектування, керування базами даних, методів комп'ютерної графіки. ПР58. Вміти **застосовувати** знання про основні принципи та методи вимірювання фізичних величин і основних технологічних параметрів для обґрунтування вибору засобів вимірювань та оцінювання їх метрологічних характеристик. ПР59. Вміти **застосовувати** знання з охорони праці в галузі професійної діяльності, основні заходи пожежної профілактики на галузевих об'єктах, систем управління охорони праці в галузі, організації робочих місць.	
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Кадрове забезпечення відповідає чинним Ліцензійним умовам провадження освітньої діяльності у сфері вищої освіти та базується на наступних принципах: відповідності наукових спеціальностей науково-педагогічних працівників освітнім галузі знань та спеціальності; обов'язковості та періодичності проходження стажування і підвищення кваліфікації викладачів; моніторингу рівня наукової активності науково-педагогічних працівників; впровадження результатів стажування та наукової діяльності в освітній процес.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення навчальних приміщень та соціальна інфраструктура університету в повному обсязі відповідає чинним Ліцензійним умовам. В освітньому процесі використовується мультимедійне обладнання для проведення лекцій, для практичних та лабораторних занять – обладнання комп'ютерних лабораторій.
Інформаційне та навчально-методичне забезпечення	Університет має власний веб-сайт за адресою http://dnu.dp.ua, де розміщено інформацію щодо інформаційного та навчально-методичного забезпечення освітнього процесу. Інформаційне забезпечення ґрунтується на використанні ресурсів: загально університетських та кафедральних бібліотек, мережі Internet з вільним доступом, колекцій цифрового репозиторію. Навчально-методичне забезпечення засновано на розроблених для кожної дисципліни робочих навчальних програмах, а також програмах практичної підготовки за спеціальністю. В наявності завдання для самостійної роботи студентів, методичні рекомендації для виконання курсових та дипломних робіт, пакети завдань для проведення ректорських робіт. Критерії оцінювання знань та вмінь студентів розроблено для поточного, семестрового та ректорського контролю з кожної дисципліни, а також для підсумкової атестації за спеціальністю.

9 – Академічна мобільність	
Національна кредитна мобільність	На загальних підставах в межах України. На основі двосторонніх договорів між ДНУ та технічними університетами України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між ДНУ та навчальними закладами країн-партнерів
Навчання іноземних здобувачів вищої освіти	Можливе, за умови вивчення курсу української мови

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 підсумкового контролю	Послідовність вивчення, семестр
1	2	3	4	5
Обов'язкові компоненти:				
І Цикл загальної підготовки				
ОК 1.1	Фізична культура	*позакредитна*	залік	2,4,5 (1 -5)
ОК 1.2	Культура України	3,0	залік	1
ОК 1.3	Безпека життєдіяльності та цивільний захист	4,0	залік	5
ОК 1.4	Філософія	3,0	екзамен	4
ОК 1.5	Українська мова за професійним спрямуванням	3,0	диф. залік	1
ОК 1.6	Іноземна мова (англійська/ німецька/ французька)	6,0	заліки	2,3
ОК 1.7	Реалізація прав, свобод і обов'язків громадянина України	3,0	залік	1
ОК 1.8	Вступ до спеціальності «Кібербезпека»	3,0	екзамен	1
ОК 1.9	Програмування в інженерних розрахунках	8,0	екзамен диф.залік	1, 2
ОК 1.10	Охорона праці в галузі	3,0	залік	7
Всього І		**36**		
ІІ Цикл професійної підготовки				
ОК 2.1	Вища математика	9,0	екзамени	1,2
ОК 2.2	Фізичні основи методів захисту інформації	8,0	залік, екзамен	2, 3
ОК 2.3	Електроніка та електротехніка	9,0	залік, екзамен	1, 2
ОК 2.4	Основи схемотехніки	6,0	екзамени	3,4
ОК 2.5	Радіотехнічні кола та сигнали	6,0	залік, диф.залік	3, 4
ОК 2.6	Курсова робота з дисципліни «Радіотехнічні кола та сигнали»	1,0	диф.залік	3
ОК 2.7	Метрологічне забезпечення засобів захисту інформації	4,0	екзамен	2
ОК 2.8	Нормативно-правове забезпечення кібербезпеки	4,0	залік	1
ОК 2.9	Організаційне забезпечення кібербезпеки	3,0	залік	2
ОК 2.10	Мікропроцесори та мікроконтролери	6,0	екзамени	3,4
ОК 2.11	Курсова робота з дисципліни «Мікропроцесори та мікроконтролери»	1,0	диф.залік	4
ОК 2.12	Бази даних та бази знань	5,0	екзамен	5
ОК 2.13	Методи та засоби захисту інформації	6,0	залік, екзамен	4, 5

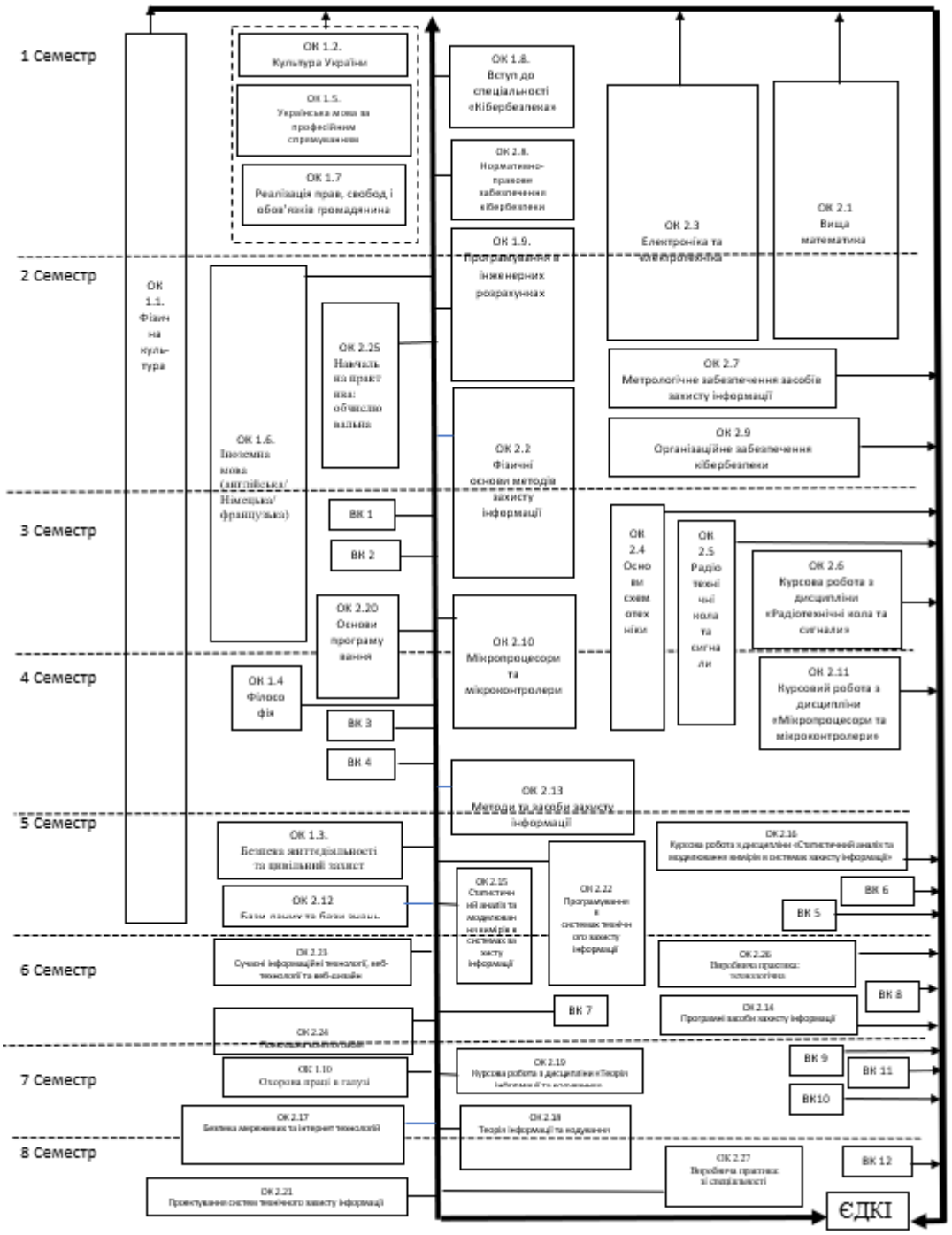
ОК 2.14	Програмні засоби захисту інформації	3,0	екзамен	6
ОК 2.15	Статистичний аналіз та моделювання вимірів в системах захисту інформації	6,0	залік, екзамен	5, 6
ОК 2.16	Курсова робота з дисципліни «Статистичний аналіз та моделювання вимірів в системах захисту інформації»	1,0	диф.залік	5
ОК 2.17	Безпека мережевих та інтернет технологій	10,0	екзамен, диф.залік	7, 8
ОК 2.18	Теорія інформації та кодування	9,0	екзамени	7,8
ОК 2.19	Курсова робота з дисципліни «Теорія інформації та кодування»	1,0	диф.залік	7
ОК 2.20	Основи програмування	8,0	екзамени	3,4
ОК 2.21	Проектування систем технічного захисту інформації	7,0	екзамен	8
ОК 2.22	Програмування в системах технічного захисту інформації	8,0	екзамени	5,6
ОК 2.23	Сучасні інформаційні технології, веб-технології та веб-дизайн	4,0	залік	6
ОК 2.24	Прикладна криптографія	7,0	залік, екзамен	6, 7
ОК 2.25	Навчальна практика: обчислювальна	3,0	диф. залік	2
ОК 2.26	Виробнича практика: технологічна	3,0	диф. залік	6
ОК 2.27	Виробнича практика: зі спеціальності	6,0	диф. залік	8
Всього II		**144**		
Всього		**180**		
Вибіркові компоненти:				
2 курс				
ВК 1	Дисципліна 1 (ВК)	5,0	диф. залік	3
ВК 2	Дисципліна 2 (ВК)	5,0	диф. залік	3
ВК 3	Дисципліна 3 (ВК)	5,0	диф. залік	4
ВК 4	Дисципліна 4 (ВК)	5,0	диф. залік	4
3 курс				
ВК 5	Дисципліна 5 (ВК)	5,0	диф. залік	5
ВК 6	Дисципліна 6 (ВК)	5,0	диф. залік	5
ВК 7	Дисципліна 7 (ВК)	5,0	диф. залік	6
ВК 8	Дисципліна 8 (ВК)	5,0	диф. залік	6
4 курс				
ВК 9	Дисципліна 9 (ВК)	5,0	диф. залік	7
ВК 10	Дисципліна 10 (ВК)	5,0	диф. залік	7
ВК 11	Дисципліна 11 (ВК)	5,0	диф. залік	7
ВК12	Дисципліна 12 (ВК)	5,0	диф. залік	8
Загальний обсяг обов'язкових компонент				**180 (75%)**
Загальний обсяг вибіркових компонент (дисциплін вибору студента)				**60 (25%)**
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ				**240**

Примітка: здобувачам вищої освіти пропонується провести вибір навчальних дисциплін на основі двох переліків вибіркових компонент:

- **університетський вибірковий каталог(УВК)**, що складається із загальноуніверситетського переліку дисциплін, на основі якого здійснюється вибір дисциплін для формування загальних компетентностей ОП, соціальних навичок та світогляду за власним уподобанням. Перелік дисциплін розміщується на сайті університету.
- **факультетський вибірковий каталог (ФВК)** – навчальні дисципліни галузево-професійного спрямування зі спеціальностей факультету, що дозволяють отримати професійні навички з певної галузі знань *та* навчальні дисципліни професійного спрямування, що дозволяють отримати поглиблену підготовку за освітньою програмою й закріплюють набуті фахові компетентності На основі засвоєння дисциплін із факультетського каталогу формуються загально-професійні або фахові компетентності. Перелік дисциплін розміщується на сайті університету/ факультету.

2.2. Структурно-логічна схема ОП

Курс	Семестр	Компоненти освітньої програми	Кількість компонентів за семестр	Кількість компонентів за навчальний рік
1	1	ОК 1.1, ОК 1.2, ОК 1.5, ОК 1.7, ОК 1.8, ОК 1.9, ОК 2.1, ОК 2.3, ОК 2.8	9	18
	2	ОК 1.1, ОК 1.6, ОК 1.9, ОК 2.1, ОК 2.2, ОК 2.3, ОК 2.7, ОК 2.9, ОК 2.25	9	
2	3	ОК 1.1, ОК 1.6, ОК 2.2,ОК 2.4, ОК 2.5, ОК 2.6, ОК 2.10, ОК 2.20, ВК 1, ВК 2	10	20
	4	ОК 1.1, ОК 1.4, ОК 2.4, ОК 2.5, ОК 2.10, ОК 2.11, ОК 2.13, ОК 2.20, ВК 3, ВК 4	10	
3	5	ОК 1.1, ОК 1.3, ОК 2.12, ОК 2.13, ОК2.15, ОК 2.16, ОК 2.22, ВК 5, ВК 6	9	17
	6	ОК 2.14, ОК 2.15, ОК2.22, ОК 2.23, ОК 2.24, ОК 2.26, ВК 7, ВК 8	8	
4	7	ОК 1.10, ОК 2.17, ОК 2.18, ОК 2.19, ОК 2.24, ВК 9, ВК 10, ВК 11,	8	13
	8	ОК 2.17, ОК 2.18, ОК 2.21, ОК 2.27, ВК 12	5	



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту
Вимоги до атестації	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом спеціальності 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти та освітньою програмою.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1.1	ОК 1.2	ОК 1.3	ОК 1.4	ОК 1.5	ОК 1.6	ОК 1.7	ОК 1.8	ОК 2.1	ОК 2.2	ОК 2.3	ОК 2.4	ОК 2.5	ОК 2.6	ОК 2.7	ОК 2.8	ОК 2.9	ОК 2.10	ОК 2.11	ОК 2.12	ОК 2.13	ОК 2.14	ОК 2.15	ОК 2.16	ОК 2.17	ОК 2.18	ОК 2.19	ОК 2.20	ОК 2.21	ОК 2.22	ОК 2.23	ОК 2.24	ОК 2.25	ОК 2.26	ОК 2.27
ЗК 1				*	*			*																										
ЗК 2		*																															*	*
ЗК 3					*	*																												*
ЗК 4																			*		*													*
ЗК 5		*														*				*						*	*	*		*		*		*	*
ЗК 6							*																												
ЗК 7	*		*																																
ФК 1																*	*																	*	*
ФК 2				*														*			*		*				*	*						*	*
ФК 3				*																		*													*
ФК 4																	*																		*
ФК 5																					*		*	*	*									*	*
ФК 6																	*													*					*
ФК 7																														*					*
ФК 8																										*				*					*
ФК 9																										*									*
ФК 10																																	*		*
ФК 11																															*	*	*	*	*
ФК 12																															*		*		*
ФК 13											*	*	*	*	*			*	*																*
ФК 14										*																									*
ФК 15									*						*					*									*						*

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

	ОК 1.1	ОК 1.2	ОК 1.3	ОК 1.4	ОК 1.5	ОК 1.6	ОК 1.7	ОК 1.8	ОК 2.1	ОК 2.2	ОК 2.3	ОК 2.4	ОК 2.5	ОК 2.6	ОК 2.7	ОК 2.8	ОК 2.9	ОК 2.10	ОК 2.11	ОК 2.12	ОК 2.13	ОК 2.14	ОК 2.15	ОК 2.16	ОК 2.17	ОК 2.18	ОК 2.19	ОК 2.20	ОК 2.21	ОК 2.22	ОК 2.23	ОК 2.24	ОК 2.25	ОК 2.26	ОК 2.27
ПР 1			*		*	*																											*	*
ПР 2																																	*	*
ПР 3		*																															*	*
ПР 4																																	*	*
ПР 5																																	*	*
ПР 6																*	*				*				*								*	
ПР 7															*	*																	*	
ПР 8																*																		
ПР 9																*																		
ПР 10				*																										*			*	*
ПР 11																								*										
ПР 12																	*																	
ПР 13																														*				
ПР 14																															*			
ПР 15																						*	*		*		*	*	*					
ПР 16																*														*				
ПР 17																								*										
ПР 18																											*							
ПР 19																								*										
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																*																	*	*
ПР 41																					*													
ПР 42																								*									*	
ПР 43																*																	*	*

	ОК 1.1	ОК 1.2	ОК 1.3	ОК 1.4	ОК 1.5	ОК 1.6	ОК 1.7	ОК 1.8	ОК 2.1	ОК 2.2	ОК 2.3	ОК 2.4	ОК 2.5	ОК 2.6	ОК 2.7	ОК 2.8	ОК 2.9	ОК 2.10	ОК 2.11	ОК 2.12	ОК 2.13	ОК 2.14	ОК 2.15	ОК 2.16	ОК 2.17	ОК 2.18	ОК 2.19	ОК 2.20	ОК 2.21	ОК 2.22	ОК 2.23	ОК 2.24	ОК 2.25	ОК 2.26	ОК 2.27
ПР 44																									*									*
ПР 45																									*									*
ПР 46																									*									*
ПР 47																																*		*
ПР 48																																*		*
ПР 49																				*					*							*		*
ПР 51																							*	*	*			*	*	*		*	*		*
ПР 52																													*	*	*				*
ПР 53																															*				*
ПР 54																														*			*		*
ПР 55	*						*																										*		*
ПР 56										*	*	*						*	*														*		*
ПР 57									*														*	*			*	*						*		*
ПР 58																													*			*		*	*
ПР 59								*							*			*	*														*		*