МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Дніпровський національний університет імені Олеся Гончара

ЗАТВЕРДЖЕНО:
Ректор Дніпровського національного університету імені Олеся Гончара
_____ Сергій ОКОВИТИЙ
«_30_» _____06_____ 2022 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 30.06.2022 р., протокол № 12

Дніпро
2022

ПЕРЕДМОВА

1. Внесено: кафедрою 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);
– від «21» грудня 2017 р. пр. №6 (редакція №2, для набору 2018/2019 н.р.);
– від «21» лютого 2019 р. пр. №9 (зміни для набору 2018/2019 н.р.);
– від «21» лютого 2019 р. пр. №9 (редакція №3, для набору 2019/2020 н.р.);
– від «10» вересня 2020 р. пр. №1 (редакція №4, для набору 2020/2021 н.р.);
– від «30» червня 2022 р., пр. №12 (редакція№5, від набору 2022/2023 н.р.);
– від «29» вересня 2024 р., пр. № 2 (редакція №5, зміни до ОП у зв'язку зі змінами до стандарту згідно з наказом МОН України від 13.06.2024 р. № 842).

3. Розробники (робоча група):
1.Клименко Світлана Володимирівна – кандидат технічних наук, доцент, доцент кафедри радіоелектронної автоматики, фізико-технічного факультету ДНУ;
2.Малайчук Валентин Павлович – доктор технічних наук, професор, завідувач кафедри радіоелектронної автоматики, фізико-технічного факультету ДНУ;
3.Петренко Олександр Миколайович – доктор технічних наук, професор, професор кафедри радіоелектронної автоматики, фізико-технічного факультету ДНУ;
4.Лисенко Наталія Олександрівна – кандидат технічних наук, доцент, доцент кафедри радіоелектронної автоматики, фізико-технічного факультету ДНУ.

4. При розробці враховані вимоги:
1. *Освітнього стандарту спеціальності:*
Стандарт вищої освіти України зі спеціальності 125 Кібербезпека для першого (бакалаврського) рівня **затверджений** наказом Міністерства освіти і науки України від 04.10 2018 р. № 1074, **вводиться в дію** з 2018/2019 навчального року.
2. *Наказу Міністерства освіти і науки України* від 13.06.2024 р. № 842 «Про внесення змін до деяких стандартів вищої освіти».

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

1. Вчена рада фізико-технічного факультету: протокол № 13 від 18.06. 2024 р.
Голова ВР ФТФ _____ *Анатолій САНІН*

2. Рада з якості ДНУ: протокол № 2 від «17» 09 2024 р.
Заступник голови РЗЯВО _____ *Валентина* СІЛІЧ-БАЛГАБАЄВА

Рецензії-відгуки стейкхолдерів

1. Роботодавці:
Данченко Дмитро Валерійович, Начальник 2-го сектору (організації технічного супроводження) Управління протидії кіберзлочинам в Дніпропетровській області ДКП НП України;

Богун Микола Олександрович, директор ТОВ «Каньйон Інжинірінг»;

Кулик Сергій Володимирович, начальник відділу технічної охорони в м. Дніпро, «Охоронний холдінг».

Мага Сергій Вікторович, фахівець Служба Безпеки України.

Артеменко Юлія Федорівна, провідний фахівець-аналітик з дослідження та моделювання ринку, ТОВ «Метал кур'єр»

Веретюк Сергій Вікторович, к.т.н., доцент, викладач кафедри комп'ютерних технологій та моделювання систем Поліський національний університет (м. Житомир), керівник інжинірингової школи Noosphere Engineering School

2. Здобувачі вищої освіти:
Сербіна Анастасія Дмитрівна, здобувач першого (бакалаврського) рівня вищої освіти, спеціальність 125 Кібербезпека, ОП «Кібербезпека», 3 курс, ДНУ;

Сокольцова Віра Сергіївна, здобувач першого (бакалаврського) рівня вищої освіти, спеціальність 125 Кібербезпека, ОП «Кібербезпека», 2 курс, ДНУ.

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	Освітньо-професійна програма «Кібербезпека»
Офіційна назва освітньої програми (англійською мовою)	Educational and professional 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	–
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 01.07.2022*р.
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
Термін дії освітньої програми	На період дії сертифікату з акредитації спеціальності (відповідно наказу МОН України від 30.10.2017 № 1432, а також *Постанови Кабінету Міністрів України від 16 березня 2022 р. № 295) або до проходження первинної акредитації освітньої програми
Інтернет-адреса постійного розміщення опису освітньої програми	www.dnu.dp.ua
2 – Мета освітньої програми	
Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та кібербезпеки. Формування та розвиток загальних і професійних компетентностей із впровадження та застосування у професійній діяльності 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 комплексних 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 проєктування. Поняття та принципи теорії автоматичного керування, систем автоматизації та комп'ютерно-інтегрованих технологій. **Методи, методики та технології:** здобувач має оволодіти методами (організаційні, технологічні, апаратні, математичні та алгоритмічні), методиками (принципів побудови систем інформаційних та технічних систем), інформаційно-комунікаційними технологіями та іншими технологіями забезпечення інформаційної та/ або кібербезпеки (наприклад, технології захисту CISCO) **Інструменти та обладнання:** Засоби захисту інформації діляться на апаратні, програмні, криптографічні та комбіновані. Таким чином, можна виділити загальні інструменти та обладнання: - системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; - комп'ютерна техніка, сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій (системні та прикладні програми, що призначені для захисту інформації), прилади та пристрої (системи управління доступом, відеокамери, датчики світла, датчику руху та ін.)
Орієнтація освітньої програми	Освітньо-професійна програма має прикладну орієнтацію. Програма інтегрує програмно-апаратні засоби 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. Дисципліни програми засновані на вивченні апаратних, програмних, криптографічних та комбінованих засобах захисту інформації; особливостях нормативних та організаційних методах захисту інформації; захисту в мережі інтернет; системах технічного захисту приміщень.
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, проєктування, 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 (Облдержадміністрація м. Дніпро, Департамент цифрової трансформації інформаційних технологій та електронного урядування; АТ АКБ «Конкорд», ТОВ «Каньйон Інжиніринг»). 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: **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 Розробники 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 Розробники обчислювальних систем 2132.2 Розробник систем захисту інформації 2139.2 Професіонали в інших галузях обчислень 2139.2 Аналітик загроз безпеки 2139.2 Аналітик з безпеки інформаційно-комунікаційних систем

	2139.2 Дізнавач (сфера кібербезпеки та захисту інформації) 2139.2 Експерт криміналіст (сфера кібербезпеки та захисту інформації) 2139.2 Експерт криміналіст судової експертизи (сфера кібербезпеки та захисту інформації) 2139.2 Фахівець з криптографічного захисту інформації 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології) 2139.2 Фахівець з підтримки інфраструктури кіберзахисту 2139.2 Фахівець з реагування на інциденти кібербезпеки 2139.2 Фахівець з тестування систем захисту інформації 2139.2 Фахівець з технічного захисту інформації 2139.2 Фахівець сфери захисту інформації 2149.2 Професіонал із організації захисту інформації з обмеженим доступом 2412 Професіонали в галузі праці та зайнятості 2412.2 Профконсультант 2423 Професіонали в галузі правоохоронної діяльності 2423 Професіонал з охоронної діяльності та безпеки 2433 Професіонали в галузі інформації та інформаційного аналізу 2433.2 Професіонали в галузі інформації та інформаційні аналітики 2433.2 Аналітик консолідованої інформації 2433.2 Інженер з науково-технічної інформації **International Standard Classification of Occupations 2008 (ISCO-08):** 2529 Security specialist (ICT).
Подальше навчання	Має право продовжити навчання на другому (магістерському) рівні для отримання освітнього ступеню магістр.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, технологія проблемного (проблемно-орієнтованого) 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, диференційовані заліки; звіти щодо виконання лабораторних робіт і практик, курсових робіт.
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. ЗК 8. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.
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 проводити 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, проєктування 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: ПР 01. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПР 02. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПР 03. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; ПР 04. 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; ПР 05. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; ПР 06. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; ПР 07. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; ПР 08. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; ПР 09. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; ПР 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; ПР 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;

	ПР 12. Розробляти моделі загроз та порушника; ПР 13. Аналізувати проєкти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; ПР 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; ПР 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; ПР 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; ПР 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; ПР 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; ПР 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; ПР 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; ПР 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; ПР 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; ПР 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; ПР 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); ПР 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; ПР 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;

	ПР 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; ПР 28. 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; ПР 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; ПР 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; ПР 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; ПР 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; ПР 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; ПР 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; ПР 35. 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; ПР 36. Виявляти небезпечні сигнали технічних засобів; ПР 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; ПР 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; ПР 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; ПР 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; ПР 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; ПР 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної, і/або кібербезпеки;

	ПР 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; ПР 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; . ПР 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; ПР 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; ПР 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; ПР 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; ПР 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; ПР 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); ПР 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; ПР 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; ПР 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. ПР 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ПР 55. Знати основи запобігання корупції, суспільної та академічної доброчесності на рівні, необхідному для формування нетерпимості до корупції та проявів недоброчесної поведінки серед здобувачів освіти та вміти застосовувати їх в професійній діяльності.
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 у 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 для проведення лекцій мультимедійне обладнання, для практичних та лабораторних занять обладнання лабораторій і спеціалізованих кабінетів, а також комп'ютерних лабораторій
Інформаційне та навчально-методичне забезпечення	Інформаційне забезпечення освітньої діяльності у Дніпровському національному університеті імені Олеся Гончара реалізується через бібліотечний фонд та використання сучасних комп'ютерних інформаційних технологій. Університет має власний веб-сайт за адресою http://dnu.dp.ua, де розміщено інформаційне та навчально-методичне забезпечення. 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 (проектів), пакети завдань для проведення ректорських та комплексних контрольних 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 основі двосторонніх договорів між Дніпровським національним університетом імені Олеся Гончара та закладами вищої освіти 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	залік	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	диф. залік	1
ОК 1.9	Інформаційні та комунікаційні технології в галузі «Кібербезпека»	3,0	залік	3
ОК 1.10	Охорона праці в галузі	3,0	екзамен	7
Всього І		**31**		
ІІ Цикл професійної підготовки				
ОК 2.1	Вища математика	9,0	екзамен	1,2
ОК 2.2	Фізичні основи методів захисту інформації	9,0	екзамен	2,3
ОК 2.3	Основи програмування	14,0	екзамен	1,2
ОК 2.4	Стандарти інформаційної та кібернетичної безпеки	4,0	екзамен	3
ОК 2.5	Комп'ютерна електроніка	7,0	екзамен	1
ОК 2.6	Курсова робота з дисципліни «Комп'ютерна електроніка»	1,0	диф.залік	1
ОК 2.7	Ризики інформаційної безпеки	4,0	екзамен	3
ОК 2.8	Нормативно-правове забезпечення кібербезпеки	5,0	залік	2
ОК 2.9	Тестування інформаційно-комунікаційних технологій	4,0	екзамен	4
ОК 2.10	Схемотехніка в системах захисту інформації	7,0	екзамен	3,4
ОК 2.11	Курсова робота з дисципліни «Схемотехніка в системах захисту інформації»	1,0	диф.залік	4
ОК 2.12	Бази даних та бази знань	4,0	екзамен	4
ОК 2.13	Методи та засоби захисту інформації	8,0	екзамен	5,6

ОК 2.14	Програмні засоби захисту інформації	8,0	залік екзамен	5, 6
ОК 2.15	Статистичний аналіз та моделювання вимірів в системах захисту інформації	8,0	залік екзамен	4, 5
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	8,0	екзамен диф.залік	7, 8
ОК 2.18	Теорія інформації та кодування	8,0	екзамен	7,8
ОК 2.19	Курсова робота з дисципліни «Теорія інформації та кодування»	1,0	диф.залік	7
ОК 2.20	Комплексні системи захисту інформації	6,0	диф.залік	8
ОК 2.21	Проєктування систем технічного захисту інформації	5,0	екзамен	8
ОК 2.22	Програмування в системах технічного захисту інформації	8,0	екзамен	5,6
ОК 2.23	Прикладна криптографія	7,0	залік екзамен	6, 7
ОК 2.24	Навчальна практика: обчислювальна	3,0	диф. залік	2
ОК 2.25	Виробнича практика: технологічна	3,0	диф. залік	6
ОК 2.26	Виробнича практика: зі спеціальності	6,0	диф. залік	8
Всього ІІ		**149**		
Всього		**180**		
Вибіркові компоненти:				
2 курс				
ВК 1	Дисципліна 1	5,0	диф. залік	3
ВК 2	Дисципліна 2	5,0	диф. залік	3
ВК 3	Дисципліна 3	5,0	диф. залік	4
ВК 4	Дисципліна 4	5,0	диф. залік	4
3 курс				
ВК 5	Дисципліна 5	5,0	диф. залік	5
ВК 6	Дисципліна 6	5,0	диф. залік	5
ВК 7	Дисципліна 7	5,0	диф. залік	6
ВК 8	Дисципліна 8	5,0	диф. залік	6
4 курс				
ВК 9	Дисципліна 9	5,0	диф. залік	7
ВК 10	Дисципліна 10	5,0	диф. залік	7
ВК 11	Дисципліна 11	5,0	диф. залік	7
ВК12	Дисципліна 12	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 2.1, ОК 2.3, ОК 2.5, ОК 2.6	9	13
	2	ОК 1.1, ОК 1.6, ОК 2.1, ОК 2.2, ОК 2.3, ОК 2.8, ОК 2.24	7	
2	3	ОК 1.1, ОК 1.6, ОК 1.9, ОК 2.2, ОК 2.4., ОК 2.7, ОК 2.10, ВК 1, ВК 2	9	16
	4	ОК 1.1, ОК 1.4, ОК 2.9, ОК 2.10, ОК 2.11, ОК 2.12, ОК2.15, ВК 3, ВК 4	9	
3	5	ОК 1.1, ОК 1.3, ОК 2.13, ОК 2.14, ОК2.15, ОК16, ОК 2.22,ВК 5, ВК 6	9	13
	6	ОК 2.13, ОК 2.14, ОК 2.22, ОК 2.23, ОК 2.25, ВК 7, ВК 8	7	
4	7	ОК 1.10, ОК 2.17, ОК 2.18, ОК 2.19, ОК 2.23, ВК 9, ВК 10, ВК 11	8	12
	8	ОК 2.17, ОК 2.18, ОК 2.20, ОК 2.21, ОК 2. 26, ВК 12	6	

Структурно-логічна схема послідовності вивчення (виконання) освітніх компонент ОП «Кібербезпека» (240 кредитів)

I курс		II курс		III курс		IV курс	
1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр
Фізична культура							
Культура України			Філософія	Безпека життєдіяльності та охорона праці в галузі			
Реалізація прав, свобод і обов'язків громадянина України		Інформаційні та комунікаційні технології в галузі «Кібербезпека»					
Українська мова за професійним спрямуванням	Іноземна мова (англійська/ німецька/ французька)						
Вступ до спеціальності «Кібербезпека»						Охорона праці в галузі	
Вища математика							
	Фізичні основи методів захисту інформації						
Основи програмування			Бази даних та бази знань				
Комп'ютерна електроніка		Ризики інформаційної безпеки					
	Нормативно-правове забезпечення кібербезпеки	Стандарти інформаційної та кібернетичної безпеки	Тестування інформаційно-комунікаційних технологій			Прикладна криптографія	
		Схемотехніка в системах захисту інформації		Методи та засоби захисту інформації		Безпека мережевих та інтернет технологій	
			Статистичний аналіз та моделювання вимірів в системах захисту інформації				Комплексні системи захисту інформації
				Програмні засоби захисту інформації		Теорія інформації та кодування	
				Програмування в системах технічного захисту інформації			Проєктування систем технічного захисту інформації
Курсова робота «Комп'ютерна електроніка»			Курсова робота з дисципліни «Схемотехніка в системах захисту інформації»	Курсова робота з дисципліни «Статистичний аналіз та моделювання вимірів в системах захисту інформації»		Курсова робота з дисципліни «Теорія інформації та кодування»	
	Навчальна практика: обчислювальна				Виробнича практика: технологічна		Виробнича практика зі спеціальності
		ВК 1	ВК 3	ВК 5	ВК 7	ВК 9	ВК 12
		ВК 2	ВК 4	ВК 6	ВК 8	ВК 10	
						ВК 11	

Позначено кольором компоненти:

Дисципліни 1 циклу	Дисципліни 1 циклу	Базові дисципліни	Фахові дисципліни з електроніки та схемотехніки	Фахові дисципліни ОП Кібербезпеки	Курсові роботи	Практики	Вибіркові компоненти

Примітка: УВК- дисципліни університетського вибіркового каталогу, ФВК- дисципліни факультетського вибіркового каталогу

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених 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 1.9	ОК 1.10	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
ЗК 1					+					+	+																							+	+	+
ЗК 2								+																											+	+
ЗК 3					+	+								+																					+	+
ЗК 4									+			+	+		+	+				+	+	+	+	+								+	+		+	+
ЗК 5											+								+		+					+		+	+				+			+	+
ЗК 6							+																													
ЗК 7	+	+	+	+						+																										
ЗК 8																							+									+				
ФК1																		+																	+	+
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 1.9	ОК 1.10	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
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															+								+													+

	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 1.9	ОК 1.10	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
ПР 40												+						+					+							+	+					+
ПР 41			+				+																				+				+				+	+
ПР 42			+									+													+			+								
ПР 43														+																						
ПР 44														+			+			+																
ПР 45														+			+																			
ПР 46														+			+																			
ПР 47																																+			+
ПР 48																																+			+
ПР 49																																			+
ПР 50																														+					+
ПР 51										+									+					+			+								
ПР 52											+																+					+		+		
ПР 53													+						+					+			+					+	+			+
ПР 54	+	+		+			+																													
ПР 55																							+								+					