МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Дніпровський національний університет імені Олеся Гончара

ЗАТВЕРДЖЕНО:
Ректор Дніпровського національного університету ім. Олеся Гончара
_____ Поляков М.В.
«_21_» _грудня_ 2017 р.

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека»

Першого рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: бакалавр, кібербезпека

Розглянуто та схвалено:
Вченою радою Дніпровського національного університету ім. Олеся Гончара від 21.12.2017 р., протокол № 6

Освітня програма вводиться в дію з 01.09.2018 р.

Дніпро
2018

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Дніпровський національний університет імені Олеся Гончара

ЗАТВЕРДЖЕНО:
Ректор Дніпровського національного університету ім. Олеся Гончара
_____ Поляков М.В.
«_21_» _лютого_ 2019 р.

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека»

Першого рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: бакалавр, кібербезпека

Розглянуто та схвалено:
Вченою радою Дніпровського національного університету ім. Олеся Гончара від 21.02.2019 р., протокол № 9

Освітня програма вводиться в дію з 01.09.2018 р.

Дніпро
2019

ПЕРЕДМОВА

1. Внесено: освітньо-професійна програма, рівень вищої освіти – перший (бакалаврський), ступінь – бакалавр, галузь знань – 12 Інформаційні технології, спеціальність – 125 Кібербезпека

2. Затверджено та надано чинності рішенням Вченої ради Дніпровського національного університету імені Олеся Гончара:

- від «21» грудня 2017 р., пр. №6 (перша редакція)
- від «21» лютого 2019 р., пр. № 9 (нова редакція) у відповідності до затвердження стандарту вищої освіти за спеціальністю 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти (наказ МОНУ №1071 від 04.10.2018р)

3. Розробники:

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.

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

4. Стандарт вищої освіти за спеціальністю 125 Кібербезпека (бакалавр) затверджено наказом МОН України №1074 від 04.10.2018р та введено в дію з 2018/2019 н.р.

2. Профіль освітньої 125 Кібербезпека

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Дніпровський національний університет імені Олеся Гончара Фізико-технічний факультет Кафедра радіоелектронної автоматики
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Бакалавр з кібербезпеки, освітня програма «Кібербезпека»
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека»
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3,10 роки
Наявність акредитації	Сертифікат про акредитацію спеціальності 125 Кібербезпека за рівнем бакалавр: серія НД № 0495177 від 19 жовтня 2017 р. Термін дії- до 1 липня 2022 р
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Повна загальна середня освіта
Мова(и) викладання	Українська мова
Термін дії освітньої програми	На період дії сертифікату акредитації спеціальності (відповідно до наказу МОН від 30.10.2017 р. №1432) або до проходження первинної акредитації ОПП
Інтернет-адреса постійного розміщення опису освітньої програми	fti.dp.ua
2 – Мета освітньої програми	
Підготовка висококваліфікованих фахівців з кібербезпеки, здатних проводити комплексні роботи с технічної охорони об’єктів.	
3 - Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності**)**	12 – Інформаційні технології 125 – Кібербезпека *Об’єкт:* 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:* 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 програма бакалавра, має прикладну орієнтацію
Основний фокус освітньої програми та спеціалізації	Спеціальна в галузі 12 Інформаційні технології, спеціальності 125 Кібербезпека. Ключові слова: комп'ютерно-інтегровані технології, інформаційні технології, система керування, система кібербезпеки, програмування.
Особливості програми	Програма передбачає обов'язковою умовою проходження навчальної та виробничої практики на передових підприємствах, що експлуатують або розробляють інформаційні технології, системи автоматизації та комп'ютерно-інтегровані технології.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть обіймати посади відповідно до Національного класифікатора України: Класифікатор професій (ДК 003:2010: технічний фахівець з інформаційних технологій, технік з автоматизації виробничих процесів, технік з метрології, технік інформаційно-обчислювального центру, технік-програміст, технік-оператор електронного устаткування, контролери та регулювальники промислових роботів).
Подальше навчання	Має право продовжити навчання на другому рівні для отримання освітнього рівня магістр.
5 – Викладання та оцінювання	
Викладання та навчання	Студенто-центроване 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, 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; -захист кваліфікаційної роботи.
6 – Програмні компетентності	
Інтегральна компетентність	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 спеціальності**:** 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.
Фахові компетентності спеціальності (ФК)	Компетентності, визначені стандартом вищої освіти спеціальності**:** ФК 8. 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 9. Здатність до використання інформаційно комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК 10. Здатність до використання програмних та програмно апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК 11. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК 12. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК 13. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК 14. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) ФК 15. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК 16. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною ФК 17. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

	ФК 18. Здатність виконувати моніторинг процесів функціонування Інформаційних, інформаційно телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК 19. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки
7 – Програмні результати навчання	
	ПР 1. застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПР 2. організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПР 3. використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; ПР 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; ПР 5. адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; ПР 6. критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; ПР 7. діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; ПР 8. готувати пропозиції до • нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; ПР 9. 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 проекти 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 ріні 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.
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 закладами освіти країн-партнерів
Навчання іноземних здобувачів вищої освіти	Можливо до 2020р. за умови вивчення української мови

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
І Цикл загальної підготовки					
Обов'язкові компоненти					
ОК 1.1	Фізична культура	8		залік	1,2,3,4,5
ОК 1.2	Філософія	3		екзамен	3
ОК 1.3	Вища математика	16		екзамен	1,2,3,4
ОК 1.4	Фізика	7		екзамен	1
ОК 1.5	Безпека життєдіяльності та охорона праці	2		залік	6
ОК 1.6	Програмування в інженерних розрахунках	10		екзамен	2,3
ОК 1.7	Радіотехнічні кола та сигнали	7		екзамен	5,6
ОК 1.8	Курсова робота з дисципліни «Радіотехнічні кола та сигнали»	1		диф.залік	5
Вибіркові компоненти					
Вибір з переліку дисциплін №1					
ВК 1	Українська мова (за професійним спрямуванням)	3		залік	2
	Культура і стилістика української фахової мови				
	Мовленнєва компетенція професійно орієнтованої особистості				
	Українське ділове мовлення				
Вибір з переліку дисциплін №2					
ВК 2	Історія України	3	6	залік	1
ВК 3	Історія українського суспільства	3			1
	Українська культура як світовий феномен	3			2
	Українська культура в контексті світової культури	3			2
	Історія української культури	3			2
	Історія та культура України	6			1,2
Вибір з переліку дисциплін №3					
ВК 4	Іноземна мова (англійська)	6		залік	1,2
	Іноземна мова (німецька)				
	Іноземна мова (французька)				
Вибір з переліку дисциплін №4					
ВК 5	Дисципліна 1	3		залік	3

ВК 6	Дисципліна 2	3	залік	4
	Політологія Соціологія Основи економіки Вибрані розділи трудового права Правознавство Релігієзнавство Основи медичних знань Екологія			
ІІ Цикл професійної підготовки				
Обов'язкові компоненти				
ОК 2.1	Архітектура комп`ютерних систем	4	диф.залік	4
ОК 2.2	Фізичні основи кібербезпеки	10	залік екзамен	3 4
ОК 2.3	Теоретичні основи електроніки	4	екзамен	4
ОК 2.4	Курсова робота з дисципліни «Теоретичні основи електроніки»	1	диф.залік	4
ОК 2.5	Теоретичні основи електротехніки	6	екзамен	2
ОК 2.6	Методи та засоби захисту інформації	4	екзамен	5
ОК 2.7	Організаційне забезпечення захисту нформації	4	залік	5
ОК 2.8	Метрологія та стандартизація	4	залік	4
ОК 2.9	Теорія інфомації та кодування	7	екзамен екзамен	7 8
ОК 2.10	Курсовий проект з дисципліни "Теорія інфомації та кодування"	2	диф.залік	7
ОК 2.11	Теорія автоматичного управління	7	залік екзамен	7 8
ОК 2.12	Основи бази даних, знань, програмування	7	екзамен екзамен	6 7
ОК 2.13	Основи теорії криптографії	7	залік екзамен	7 8
ОК 2.14	Приймально-передавальні пристрої систем технічного захисту інформації	7	екзамен екзамен	6 7
ОК 2.15	Вступ до спеціальності	4	екзамен	1
ОК 2.16	Інженерна та комп'ютерна графіка	6	екзамен	1
ОК 2.17	Сучасні інформаційні технології прийняття рішень	6	екзамен	3
ОК 2.18	Технологія приладобудування	4	залік	5
ОК 2.19	Безпека мережевих та інтернет-технологій	4	екзамен	5
ОК 2.20	Статистичний аналіз та моделювання вимірів	6	екзамен залік	5 6

ОК 2.21	Курсова робота з дисципліни "Статистичний аналіз та моделювання вимірів"	1	диф.залік	6
ОК 2.22	Навчальна практика: обчислювальна	3	диф.залік	2
ОК 2.23	Виробнича практика: технологічна	3	диф.залік	6
ОК 2.24	Виробнича практика: переддипломна	6	диф.залік	8
ОК 2.25	Виконання дипломної роботи	6	Захист дипломної роботи	8
ОК 2.26	Атестація	3		8
Вибіркові компоненти				
Вибір з переліку дисциплін №5				
ВК7	Основи схемотехніки цифрових пристроїв Комп'ютерна схемотехніка Інформаційно-вимірювальні комплекси	9	залік	3,4
Вибір з переліку дисциплін №6				
ВК8	Цифрова обробка та передача інформації Основи цифрової обробки сигналів та зображень Фізична культура	7	залік	6,7
Вибір з переліку дисциплін №7				
ВК9	Основи тестування програмного забезпечення в задачах кібербезпеки Комп'ютерні технології та програмування	10	залік	5,6
Вибір з переліку дисциплін №8				
ВК 10	Основи теорії ризиків Аналіз і управління ризиками в інформаційній безпеці	6	залік	7,8
Вибір з переліку дисциплін №9				
ВК 11	Проектування комплексних систем захисту інформації Системи автоматизованого проектування CAD/CAM/CAE	7	залік	7,8
Загальний обсяг обов'язкових компонент				**180 (75%)**
Загальний обсяг вибіркових компонент (дисциплін вибору студента)				**60 (25%)**
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ				**240**

Структурно-логічна схема ОП

Курс	Семестр	Компоненти освітньої програми	Кількість компонентів за семестр	Кількість компонентів за навчальний рік
1	1	ОК1.3, ОК1.4, ОК2.16, ОК2.17, ВК3, ВК4	6	14
	2	ОК1.1, ОК1.3, ОК1.6, ОК2.5, ОК2.20, ОК2.23, ВК1, ВК2	8	
2	3	ОК1.2, ОК1.3, ОК1.6, ОК2.2, ОК2.18, ВК5, ВК7	7	16
	4	ОК1.1, ОК1.3, ОК2.1, ОК2.2, ОК2.3 (ОК2.4), ОК 2.8, ВК6, ВК 7	9	
3	5	ОК1.1, ОК1.7, (ОК1,8) , ОК2.6, ОК2.7, ОК 2.19, ОК2.20, ОК2.21, ВК9	9	18
	6	ОК1.5, ОК1.7, ОК2.13, ОК2.15, ОК2.22, ОК2.24,ОК2.21, ВК8, ВК9	9	
4	7	ОК2.9(ОК2.10), ОК2.11, ОК2.12, ОК2.13, ОК2.14, ОК2.15, ВК8, ВК10,ВК11	10	18
	8	ОК2.9, ОК2.11, ОК2.12, ОК2.14, ОК2.25, ОК2.26, ВК10, ВК11	8	

5. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація проводиться у формі публічного захисту кваліфікаційної роботи – дипломної роботи бакалавра.
Вимоги до кваліфікаційної роботи	До атестації допускають здобувачів вищої освіти, які успішно завершили теоретичний курс навчання та виконали всі види практичної підготовки, передбачені навчальним планом. Кваліфікаційна робота передбачає розв'язання складного спеціалізованого завдання або практичної проблеми, із застосуванням теорій та методів спеціальності, що характеризуються комплексністю та невизначеністю умов, під час професійної діяльності у галузі автоматизації. Кваліфікаційна робота має бути перевірена на плагіат. Кваліфікаційна робота має бути оприлюднена на офіційному сайті ДНУ імені Олеся Гончара або у репозитарії університету. Атестація здійснюється відкрито і публічно.

5. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК1.1	ОК1.2	ОК1.3	ОК1.4	ОК1.5	ОК1.6	ОК1.7	ОК1.8	ОК2.1	ОК2.2	ОК2.3	ОК2.4	ОК2.5	ОК2.6	ОК2.7	ОК2.8	ОК2.9	ОК2.10	ОК2.11	ОК2.12	ОК2.13	ОК2.14	ОК2.15	ОК2.16	ОК2.17	ОК2.18	ОК2.19	ОК2.20	ОК2.21	ОК22.2	ОК2.23	ОК2.24	ОК2.25	ОК2.26	ОК2.27	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК8	ВК9	ВК10	ВК11
ЗК1			+	+																																									
ЗК2		+	+																																+											
ЗК3																																					+									
ЗК4					+	+	+	+	+	+	+		+		+	+	+	+	+		+	+	+	+	+	+		+	+	+	+	+	+	+							+	+	+	+	+
ЗК5		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+											
ЗК6					+	+																														+	+								
ЗК7					+	+																														+	+		+	+					
ФК8			+																							+	+				+														
ФК9										+	+	+	+	+		+			+												+												+	+
ФК10											+											+																						+	+	+
ФК11																		+	+	+		+				+	+				+												+	+			
ФК12												+			+			+				+		+					+	+												+			+	+
ФК13								+										+			+		+		+				+	+	+												+	+		
ФК14					+	+										+		+			+																									
ФК15																																							+	+						
ФК16					+	+																	+																				+			
ФК17					+	+																	+																+						
ФК18					+	+																									+					+	+							
ФК19																															+					+	+							

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

	ОК1.1	ОК1.2	ОК1.3	ОК1.4	ОК1.5	ОК1.6	ОК1.7	ОК1.8	ОК2.1	ОК2.2	ОК2.3	ОК2.4	ОК2.5	ОК2.6	ОК2.7	ОК2.8	ОК2.9	ОК2.10	ОК2.11	ОК2.12	ОК2.13	ОК2.14	ОК2.15	ОК2.16	ОК2.17	ОК2.18	ОК2.19	ОК2.20	ОК2.21	ОК22.2	ОК2.23	ОК2.24	ОК2.25	ОК2.26	ОК2.27	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК8	ВК9	ВК10	ВК11
ПР1			+	+																																									
ПР2		+	+																																+											
ПР3																																					+									
ПР4					+	+	+	+	+	+	+		+		+	+	+	+	+		+	+	+	+	+	+		+	+	+	+	+	+	+							+	+	+	+	+
ПР5		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+											
ПР6					+	+																														+	+								
ПР7					+	+																														+	+		+	+					
ПР8			+																							+	+				+														
ПР9										+	+	+	+	+		+			+												+											+	+
ПР10											+											+																					+	+	+
ПР11																		+	+	+		+				+	+				+											+	+			
ПР12												+			+			+				+		+					+	+											+			+	+
ПР13								+										+			+		+		+				+	+	+												+	+		
ПР14					+	+										+		+			+																									
ПР15																																							+	+						
ПР16					+	+																	+																				+			
ПР17	+																																+	+												
ПР18		+																																												
ПР19			+																																											
ПР20			+																																											
ПР21			+						+		+	+																+																	
ПР22			+					+														+										+													
ПР23			+								+							+									+						+	+											

ПР24			+	+	+	+	+			+							+	+																										+	+	
ПР25			+								+	+										+						+										+		+						
ПР26		+	+	+	+	+			+							+	+																										+	+		
ПР27			+													+									+														+							
ПР28			+		+			+				+																		+		+														
ПР29			+		+							+												+		+										+			+				+			
ПР30	+		+									+																																	+	+
ПР31			+									+	+											+						+							+									+
ПР32		+	+	+	+	+			+							+	+																					+					+	+		
ПР33			+										+				+	+					+																							
ПР34			+						+					+									+																							
ПР35			+							+			+										+				+							+	+						+					
ПР36			+							+		+								+					+							+														
ПР37																																	+													
ПР38																					+												+													
ПР39																						+											+													
ПР40	+	+	+		+						+																																			+
ПР41			+								+	+							+																											
ПР42			+								+																	+													+					
ПР43			+										+																					+	+											
ПР44			+							+			+								+																		+							
ПР45			+										+																+																	
ПР46		+	+	+	+	+			+							+	+																										+	+		
ПР47												+																			+															

ПР48			+										+			+																														
ПР49			+								+	+						+	+				+							+		+									+					
ПР50			+								+		+				+												+					+										+		
ПР51			+									+	+																																	
ПР52			+										+			+					+	+														+										
ПР53			+									+	+						+																											
ПР54			+										+																							+										+

Зміни до ОПП для набору 2019/20 н.р.

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
І Цикл загальної підготовки					
Обов'язкові компоненти					
ОК 1.1	Фізична культура	8		залік	1,2,3,4,5
ОК 1.2	Філософія	3		екзамен	3
ОК 1.3	Вища математика	16		екзамен	1,2,3,4
ОК 1.4	Фізика	7		екзамен	1
ОК 1.5	Безпека життєдіяльності та охорона праці	2		залік	6
ОК 1.6	Програмування в задачах кібербезпеки	10		екзамен	2,3
ОК 1.7	Радіотехнічні кола та сигнали	7		екзамен	5,6
ОК 1.8	Курсова робота з дисципліни «Радіотехнічні кола та сигнали»	1		диф.залік	5
Вибіркові компоненти					
Вибір з переліку дисциплін №1					
ВК 1	Українська мова (за професійним спрямуванням)	3		залік	2
	Культура і стилістика української фахової мови				
	Мовленнєва компетенція професійно орієнтованої особистості				
	Українське ділове мовлення				
Вибір з переліку дисциплін №2					
ВК 2	Історія України	3	6	залік	2
ВК 3	Історія українського суспільства	3			2
	Українська культура як світовий феномен	3			1
	Українська культура в контексті світової культури	3			1
	Історія української культури	3			1
	Історія та культура України	6			1,2
Вибір з переліку дисциплін №3					
ВК 4	Іноземна мова (англійська)	6		залік	1,2

	Іноземна мова (німецька) Іноземна мова (французька)			
Вибір з переліку дисциплін №4				
ВК 5	Дисципліна 1	3	залік	3
ВК 6	Дисципліна 2	3	залік	4
	Політологія Соціологія Основи економіки Вибрані розділи трудового права Правознавство Релігієзнавство Основи медичних знань Екологія			
ІІ Цикл професійної підготовки				
Обов'язкові компоненти				
ОК 2.1	Архітектура комп`ютерних систем	4	диф.залік	4
ОК 2.2	Фізичні основи кібербезпеки	10	залік екзамен	3 4
ОК 2.3	Теоретичні основи електроніки	4	екзамен	4
ОК 2.4	Курсова робота з дисципліни «Теоретичні основи електроніки»	1	диф.залік	4
ОК 2.5	Теоретичні основи електротехніки	6	екзамен	2
ОК 2.6	Методи та засоби захисту інформації	4	екзамен	5
ОК 2.7	Організаційне забезпечення захисту нформації	4	залік	5
ОК 2.8	Метрологія та стандартизація	4	залік	4
ОК 2.9	Теорія інфомації та кодування	7	екзамен екзамен	7 8
ОК 2.10	Курсовий проект з дисципліни "Теорія інфомації та кодування"	2	диф.залік	7
ОК 2.11	Теорія автоматичного управління	7	залік екзамен	7 8
ОК 2.12	Основи бази даних, знань, програмування	7	екзамен екзамен	6 7
ОК 2.13	Основи теорії криптографії	7	залік екзамен	7 8
ОК 2.14	Приймально-передавальні пристрої систем технічного захисту інформації	7	екзамен екзамен	6 7
ОК 2.15	Вступ до спеціальності	4	екзамен	1
ОК 2.16	Інженерна та комп'ютерна графіка	6	екзамен	1
ОК 2.17	Сучасні інформаційні технології прийняття рішень	6	екзамен	3
ОК 2.18	Технологія приладобудування	4	залік	5

ОК 2.19	Безпека мережевих та інтернет-технологій	4	екзамен	5
ОК 2.20	Статистичний аналіз та моделювання вимірів	6	екзамен залік	5 6
ОК 2.21	Курсова робота з дисципліни "Статистичний аналіз та моделювання вимірів"	1	диф.залік	6
ОК 2.22	Навчальна практика: обчислювальна	3	диф.залік	2
ОК 2.23	Виробнича практика: технологічна	3	диф.залік	6
ОК 2.24	Виробнича практика: переддипломна	6	диф.залік	8
ОК 2.25	Підготовка та захист кваліфікаційної роботи	9	Захист кваліфікаційної роботи	8
Вибіркові компоненти				
Вибір з переліку дисциплін №5				
ВК7	Основи схемотехніки цифрових пристроїв Комп'ютерна схемотехніка Інформаційно-вимірювальні комплекси	9	залік	3,4
Вибір з переліку дисциплін №6				
ВК8	Цифрова обробка та передача інформації Основи цифрової обробки сигналів та зображень Фізична культура	7	залік	6,7
Вибір з переліку дисциплін №7				
ВК9	Основи тестування програмного забезпечення в задачах кібербезпеки Комп'ютерні технології та програмування	10	залік	5,6
Вибір з переліку дисциплін №8				
ВК 10	Основи теорії ризиків Аналіз і управління ризиками в інформаційній безпеці Іноземна мова	6	залік	7,8
Вибір з переліку дисциплін №9				
ВК 11	Проектування комплексних систем захисту інформації Системи автоматизованого проектування CAD/CAM/CAE	7	залік	7,8
Загальний обсяг обов'язкових компонент				**180 (75%)**
Загальний обсяг вибіркових компонент (дисциплін вибору студента)				**60 (25%)**
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ				**240**

Структурно-логічна схема ОП

Курс	Семестр	Компоненти освітньої програми	Кількість компонентів за семестр	Кількість компонентів за навчальний рік
1	1	ОК1.3, ОК1.4, ОК2.16, ОК2.17, ВК3, ВК4	6	14
	2	ОК1.1, ОК1.3, ОК1.6, ОК2.5, ОК2.20, ОК2.23, ВК1, ВК2	8	
2	3	ОК1.2, ОК1.3, ОК1.6, ОК2.2, ОК2.18, ВК5, ВК7	7	16
	4	ОК1.1, ОК1.3, ОК2.1, ОК2.2, ОК2.3 (ОК2.4), ОК 2.8, ВК6, ВК 7	9	
3	5	ОК1.1, ОК1.7, (ОК1,8) , ОК2.6, ОК2.7, ОК 2.19, ОК2.20, ОК2.21, ВК9	9	18
	6	ОК1.5, ОК1.7, ОК2.13, ОК2.15, ОК2.22, ОК2.24,ОК2.21, ВК8, ВК9	9	
4	7	ОК2.9(ОК2.10), ОК2.11, ОК2.12, ОК2.13, ОК2.14, ОК2.15, ВК8, ВК10,ВК11	10	18
	8	ОК2.9, ОК2.11, ОК2.12, ОК2.14, ОК2.25, ОК2.26, ВК10, ВК11	8	

5. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація проводиться у формі публічного захисту кваліфікаційної роботи – дипломної роботи бакалавра.
Вимоги до кваліфікаційної роботи	До атестації допускають здобувачів вищої освіти, які успішно завершили теоретичний курс навчання та виконали всі види практичної підготовки, передбачені навчальним планом. Кваліфікаційна робота передбачає розв'язання складного спеціалізованого завдання або практичної проблеми, із застосуванням теорій та методів спеціальності, що характеризуються комплексністю та невизначеністю умов, під час професійної діяльності у галузі автоматизації. Кваліфікаційна робота має бути перевірена на плагіат. Кваліфікаційна робота має бути оприлюднена на офіційному сайті ДНУ імені Олеся Гончара або у репозитарії університету. Атестація здійснюється відкрито і публічно.

6. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК1.1	ОК1.2	ОК1.3	ОК1.4	ОК1.5	ОК1.6	ОК1.7	ОК1.8	ОК2.1	ОК2.2	ОК2.3	ОК2.4	ОК2.5	ОК2.6	ОК2.7	ОК2.8	ОК2.9	ОК2.10	ОК2.11	ОК2.12	ОК2.13	ОК2.14	ОК2.15	ОК2.16	ОК2.17	ОК2.18	ОК2.19	ОК2.20	ОК2.21	ОК22.2	ОК2.23	ОК2.24	ОК2.25	ОК2.26	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК8	ВК9	ВК10	ВК11
ЗК1			+	+																																								
ЗК2		+	+																															+										
ЗК3																																				+								
ЗК4					+	+	+	+	+	+	+		+		+	+	+	+	+		+	+	+	+	+	+		+	+	+	+	+	+						+	+	+	+	+
ЗК5		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+											
ЗК6					+	+																													+	+								
ЗК7					+	+																													+	+		+	+					
ФК8			+																						+	+				+													
ФК9										+	+	+	+	+		+			+											+											+	+
ФК10											+											+																				+	+	+
ФК11																		+	+	+		+				+	+			+											+	+		
ФК12												+			+			+				+		+					+	+											+		+	+
ФК13								+										+			+		+		+				+	+	+											+	+		
ФК14					+	+										+		+			+																							
ФК15																																						+	+					
ФК16					+	+																	+																		+			
ФК17					+	+																	+															+					
ФК18					+	+																								+					+	+							
ФК19																														+					+	+							

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

	ОК1.1	ОК1.2	ОК1.3	ОК1.4	ОК1.5	ОК1.6	ОК1.7	ОК1.8	ОК2.1	ОК2.2	ОК2.3	ОК2.4	ОК2.5	ОК2.6	ОК2.7	ОК2.8	ОК2.9	ОК2.10	ОК2.11	ОК2.12	ОК2.13	ОК2.14	ОК2.15	ОК2.16	ОК2.17	ОК2.18	ОК2.19	ОК2.20	ОК2.21	ОК22.2	ОК2.23	ОК2.24	ОК2.25	ОК2.26	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК8	ВК9	ВК10	ВК11
ПР1			+	+																																								
ПР2		+	+																															+										
ПР3																																				+								
ПР4					+	+	+	+	+	+	+		+		+	+	+	+	+		+	+	+	+	+	+		+	+	+	+	+	+							+	+	+	+	+
ПР5		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+											
ПР6					+	+																													+	+									
ПР7					+	+																													+	+		+	+						
ПР8			+																							+	+				+													
ПР9										+	+	+	+	+		+			+												+										+	+	
ПР10											+												+																				+	+	+
ПР11																		+	+	+		+				+	+				+											+	+		
ПР12												+			+			+				+		+					+	+											+			+	+
ПР13								+										+			+		+		+				+	+	+											+	+		
ПР14					+	+										+		+			+																								
ПР15																																					+	+						
ПР16					+	+																	+																			+			
ПР17	+																																												
ПР18		+																																											
ПР19			+																																										
ПР20			+																																										
ПР21			+						+		+	+																+																
ПР22			+					+														+										+												
ПР23			+								+							+									+						+											

ПР24			+	+	+	+	+			+							+	+																											
ПР25			+								+	+											+																					
ПР26		+	+	+	+	+			+								+	+																								+	+		
ПР27			+														+											+																	
ПР28			+		+			+				+																			+		+										
ПР29			+		+							+														+		+								+						+			
ПР30	+		+									+																														+	+	
ПР31			+									+	+												+																		+	
ПР32		+	+	+	+	+			+								+	+																								+	+		
ПР33			+										+					+	+						+																				
ПР34			+						+					+											+																				
ПР35			+							+			+												+																				
ПР36			+							+		+														+																			
ПР37																																													
ПР38																																													
ПР39																																													
ПР40	+	+	+		+						+																																+	
ПР41			+								+	+								+																								
ПР42			+								+																	+																
ПР43			+										+																																
ПР44			+							+			+										+																					
ПР45			+										+																	+														
ПР46		+	+	+	+	+			+								+	+																								+	+		
ПР47												+																				+												

ПР48			+										+			+																													
ПР49			+								+	+						+	+				+							+		+								+					
ПР50			+								+		+				+												+					+									+		
ПР51			+									+	+																																
ПР52			+										+			+					+	+													+										
ПР53			+									+	+						+																										
ПР54			+										+																						+										+