МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ НАУКИ І ТЕХНОЛОГІЙ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

назва «Кібербезпека»

першого (бакалаврського) рівня вищої освіти

спеціальність 125 Кібербезпека

галузь знань 12 Інформаційні технології

кваліфікація Бакалавр з кібербезпеки

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради, професор

_____ Олександр ПШІНЬКО

«28» грудня 2021р. протокол № 3

Освітня програма вводиться в дію

з «28» грудня 2021р.

В.о. ректора _____ Олександр ПШІНЬКО

Наказ № 43 від «28» грудня 2021р.

Дніпро–2021

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми
першого (бакалаврського) рівня вищої освіти

«Кібербезпека»
(назва освітньо-професійної програми)

Перший проректор _____ Анатолій РАДКЕВИЧ
Підпис Ім'я, прізвище
«28» 12 2021р.

Навчальний відділ
Начальник НВ _____ Людмила АНДРАШКО
Підпис Ім'я, прізвище
«28» 12 2021р.

Навчально-методичний відділ
Начальник НМВ _____ Сергій ГРИШЕЧКІН
Підпис Ім'я, прізвище
«28» 12 2021р.

ПЕРЕДМОВА

освітньо-професійної програми

«Кібербезпека»

першого (бакалаврського) рівня вищої освіти

ВНЕСЕНО

Кафедрою «Електронні обчислювальні машини»

«10» грудня 2021р. протокол № 5

Завідувач кафедри _____ Ігор ЖУКОВИЦЬКИЙ

Підпис Ім'я, прізвище

ПІДСТАВА

Програму складено на підставі стандарту вищої освіти за спеціальністю 125 «Кібербезпека», що затверджений наказом МОН України від 04.10.2018р. №1074 та відповідно до наказу МОН України від 26.04.2021р. №464 «Про утворення Українського державного університету науки і технологій» з метою продовження реалізації ОПП «Кібербезпека» ДНУЗТ/НМетАУ після реорганізації в УДУНТ.

Розробники програми:

1. Д. Остапець, к.т.н., доцент, доцент каф. ЕОМ – гарант _____
   Ім'я, прізвище, науковий ступінь, звання підпис
2. І. Жуковицький, д.т.н, профеор, зав. кафедрою ЕОМ _____
   Ім'я, прізвище, науковий ступінь, звання підпис
3. В. Пахомова, к.т.н., доцент, доцент каф. ЕОМ _____
   Ім'я, прізвище, науковий ступінь, звання підпис
4. Г. Тараскін, головний інженер ВП «ДВ» філії «ГІОЦ» АТ «УЗ» _____
   Ім'я, прізвище, науковий ступінь, звання підпис
5. Б. Кушнір, студент групи КБ20120 _____
   Ім'я, прізвище, науковий ступінь, звання підпис

До ОПП надані такі рецензії-відгуки

1. А. Гиря – Начальник виробничого підрозділу «Дніпровське відділення» філії «Головний ІОЦ» АТ «Укрзалізниця»
2. С. Чепіжко – Заступник директора філії «ПКТБ ІТ» АТ «Укрзалізниця»
3. Д. Ярьоменко – студент групи КБ1811

1. Профіль освітньо-професійної програми
спеціальність 125 Кібербезпека
назва «Кібербезпека»

1.1 - Загальна інформація	
Повна назва закладу вищої освіти	Український державний університет науки і технологій
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Кваліфікація – Бакалавр з Кібербезпеки
Офіційна назва освітньої програми	ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА «Кібербезпека» першого (бакалаврського) рівня вищої освіти Галузь знань 12 Інформаційні технології Спеціальність 125 Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний. Обсяг освітньої програми бакалавра: - на базі повної загальної середньої освіти – 240 кредитів ЄКТС - на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста). На основі ступеня «фаховий молодший бакалавр» заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти. Прийом на основі ступенів «молодший бакалавр», «фаховий молодший бакалавр» або освітньо-кваліфікаційного рівня «молодший спеціаліст» здійснюється за результатами зовнішнього незалежного оцінювання в порядку, визначеному законодавством.
Наявність акредитації	Міністерство освіти і науки України, ДОУ «Навчально-методичний центр з питань якості освіти», сертифікат УД №04016429.
Рівень	НРК України - 6 рівень / перший (бакалаврський) рівень вищої освіти
Передумови	Вимоги щодо попередньої освіти: – Повна загальна середня освіта або ступінь «молодший бакалавр» (освітньо-кваліфікаційний рівень «молодший спеціаліст») – Решта вимог визначаються правилами прийому на освітньо-професійну програму бакалавра
Мова(и) викладання	Українська мова
Термін дії освітньої програми	До 01.07.2029р, щорічний моніторинг
Інтернет-адреса постійного розміщення опису освітньої програми	http://pk.diit.edu.ua/?view=static&id=6
1.2 - Мета освітньої програми	
Мета (цілі) освітньої програми: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, забезпечення високого	

рівня підготовки фахівців та формування особистості фахівця, здатного вирішувати типові та складні професійні завдання в галузі інформаційної та/або кібербезпеки. Дана ОПП корелюється зі Стратегічним планом розвитку університету щодо місії університету (зокрема, у частині підготовки висококваліфікованих фахівців, яких визнано в Україні та за її межами).	
1.3 - Характеристика освітньої програми	
Опис предметної області	**Об'єкти професійної діяльності випускників:** – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. **Цілі навчання:** підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області:** **Знання:** – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. **Методи, методики та технології:** Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. **Інструменти та обладнання:** – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	**Освітньо-професійна** **Види професійної діяльності**, до виконання яких готуються випускники, що освоїли програму бакалавра: проектно-технологічна; виробничо-технологічна; організаційно-управлінська; науково-дослідна; інноваційна
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта в галузі «**Інформаційні технології»** за спеціальністю **«Кібербезпека».** Ключові слова:

<table>
<tr><td></td><td>– Апаратні засоби забезпечення безпеки комп’ютерних систем;
– Програмні засоби забезпечення безпеки комп’ютерних систем;
– Інформаційна безпека комп’ютерних систем та мереж.</td></tr>
<tr><td>Особливості програми</td><td>Підготовка висококваліфікованих фахівців для роботи в галузі 12 «Інформаційні технології», враховуючи потреби організацій, промислових підприємств, підприємств транспорту, науково-дослідних та освітніх закладів Придніпровського регіону, України та інших країн.
Системний підхід до підготовки бакалаврів, інтеграції класичних методів освіти та практичного досвіду.</td></tr>
<tr><td colspan="2">1.4. Придатність випускників до працевлаштування та подальшого навчання</td></tr>
<tr><td>Придатність до працевлаштування</td><td>Назви професій згідно з Національним класифікатором професій України (ДК 003:2010):<table>
<tr><td>3</td><td>Фахівці</td></tr>
<tr><td>31</td><td>Технічні фахівці в галузі прикладних наук та техніки</td></tr>
<tr><td>312</td><td>Технічні фахівці в галузі обчислювальної техніки</td></tr>
<tr><td>3121</td><td>Техніки-програмісти</td></tr>
<tr><td>3123</td><td>Контролери та регулювальники промислових роботів</td></tr>
<tr><td>3114</td><td>Технік із конфігурованої комп'ютерної системи</td></tr>
<tr><td>3114</td><td>24947 Технік обчислювального (інформаційно-обчислювального) центру</td></tr>
<tr><td>3114</td><td>24971 Технік-конструктор (електроніка)</td></tr>
<tr><td>3114</td><td>25041 Технік-технолог (електроніка)</td></tr>
<tr><td>3114</td><td>Фахівець інфокомунікацій</td></tr>
<tr><td>3121</td><td>25036 Технік-програміст</td></tr>
<tr><td>3121</td><td>Фахівець з інформаційних технологій</td></tr>
<tr><td>3121</td><td>Фахівець з комп'ютерної графіки (дизайну)</td></tr>
<tr><td>3121</td><td>Фахівець з розробки та тестування програмного забезпечення</td></tr>
<tr><td>3121</td><td>Фахівець з розроблення комп'ютерних програм</td></tr>
</table></td></tr>
<tr><td>Подальше навчання</td><td>Мають право продовжити навчання на другому (магістерському) рівні за цією та іншими освітніми програмами.</td></tr>
<tr><td colspan="2">1.5. Викладання та оцінювання</td></tr>
<tr><td>Викладання та навчання</td><td>Студентоцентроване навчання, проблемно–орієнтоване навчання, самонавчання на основі інформаційних технологій дистанційного навчання. Основними формами організації навчального процесу є лекції, мультимедійні лекції, семінари, практичні заняття, лабораторні роботи, консультації, курсове проектування, самостійна робота (зокрема, з використанням технології дистанційного online навчання), виробнича практика, підготовка та захист кваліфікаційної бакалаврської роботи.</td></tr>
<tr><td>Оцінювання</td><td>Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль.
Форми контролю: усне та письмове опитування, тестові завдання, захист лабораторних та практичних робіт, захисти курсових</td></tr>
</table>

	проектів та робіт, захист кваліфікаційної роботи, єдиний державний кваліфікаційний іспит.
1.6. 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 (КЗ)	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. Здатність 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. КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Фахові компетентності спеціальності (КФ)	КФ 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. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси

	нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
1.7. Програмні результати навчання (ПР)	
	ПР1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПР2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПР3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; ПР4. 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; ПР5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; ПР6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; ПР7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; ПР8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; ПР9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; ПР10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; ПР11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; ПР12. Розробляти моделі загроз та порушника;

	ПР13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; ПР14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; ПР15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; ПР16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; ПР17. 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; ПР18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; ПР19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; ПР20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; ПР21. 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; ПР22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки; ПР23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; ПР24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно - телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); ПР25. 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; ПР26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; ПР27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; ПР28. 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; ПР29. 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; ПР30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; ПР31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; ПР32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; ПР33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; ПР34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; ПР35. 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; ПР36. Виявляти небезпечні сигнали технічних засобів; ПР37. 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; ПР38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;

	ПР39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; ПР40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; ПР41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; ПР42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; ПР43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; ПР44. 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; ПР45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; ПР46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; ПР47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; ПР48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; ПР49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; ПР50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); ПР51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; ПР52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; ПР53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз; ПР54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого

	розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
1.8. Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідає ліцензійним умовам згідно з Постановою КМУ від 10.12.15 №1187 (в редакції постанови КМУ від 24.03.21 №365). Кадровий склад науково-педагогічних, педагогічних працівників, що забезпечує навчальний процес на здобуття студентами першого (бакалаврського) рівня вищої освіти за освітньою програмою: доктори наук, професори – 28%, кандидати наук, доценти – 72%.
Матеріально-технічне забезпечення	Лекційні аудиторії, що мають мультимедійне обладнання; Лабораторії, що мають обладнання, яке відповідає предметній галузі (вимірювальні пристрої, комп'ютери, мережеве обладнання, стенди, тощо). Перелік обладнання та приміщень, де воно розташовано, вказано на сайті університету: http://diit.edu.ua/faculty/tk/kafedra/evm/material_base Відповідно договорам про філії кафедри ЕОМ (виробничій підрозділ «Дніпровського відділення» філії «Головний інформаційно-обчислювальний центр», філії «Проектно-конструкторське технологічне бюро інформаційних технологій» АТ «Українська залізниця», лабораторії спецзв'язку та захисту інформації першого відділку «Дніпровського відділення» АТ «Українська залізниця») можливо використання лабораторій цих підприємств в начальному процесі кафедри. У цілому матеріально-технічне забезпечення освітнього процесу відповідає ліцензійним умовам згідно з Постановою КМУ від 10.12.15 №1187 (в редакції постанови КМУ від 24.03.21 №365).
Інформаційне та навчально-методичне забезпечення	**Інформаційно-технологічне забезпечення освітнього процесу** Бібліотека: – використання бібліотечного фонду університету, онлайн-ресурсів та баз даних; – інформаційне забезпечення студентів, які працюють над проектами та дипломами Навчальні ресурси: – довгострокові і короткострокові позики книг, доступ до онлайн-ресурсів, міжбібліотечні позики, відеотека; – продовження терміну позики та бронювання книг онлайн; – доступ до електронних журналів; – доступ до електронних бібліотечних ресурсів світу; – доступ до електронного навчального середовища Moodle; – технологічне і матеріально-технічне забезпечення освітнього процесу Академічна підтримка: – консультації з вибору програми, окремих вибіркових дисциплін, – проектування індивідуальних навчальних траєкторій – персональне консультування
1.9. Академічна мобільність	
Національна кредитна мобільність	Національна кредитна мобільність регламентується «Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу», затвердженого наказом ректора.

Міжнародна кредитна мобільність	Міжнародна кредитна мобільність здійснюється на основі договорів між іноземними університетами та УДУНТ і регламентується «Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу», затвердженого наказом ректора.
Навчання іноземних здобувачів вищої освіти	Підготовка іноземців здійснюється згідно із Законами 15 здобувачів вищої освіти України «Про вищу освіту», «Про правовий статус іноземців та осіб без громадянства», постановами Кабінету Міністрів України від 26 лютого 1993 року № 136 «Про навчання іноземних громадян в Україні», від 11 вересня 2013 року № 684 «Деякі питання набору для навчання іноземців та осіб без громадянства», наказом Міністерства освіти і науки України від 01 листопада 2013 року № 1541 «Деякі питання організації набору та навчання (стажування) іноземців та осіб без громадянства», зареєстрованим у Міністерстві юстиції України 25 листопада 2013 року № 2004/24536. Наявність в університеті відділу міжнародних зав'язків, відділу роботи з іноземними студентами, гуртожитку та інформаційного пакету для іноземних студентів.

2. Перелік компонентів освітньо-професійної програми та її логічна послідовність

2.1 Перелік компонентів ОП

Код освітньої компоненти	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. Обов'язкові компоненти (ОК)			
1.1. Обов'язкові компоненти загальної підготовки			
ОК1	Історія і культура України	5	Екзамен
ОК2	Українська мова (за професійним спрямуванням)	3	Залік
ОК3	Іноземна мова	9	Екзамен
ОК4	Фізичне виховання*	14*	Залік
ОК5	Вища математика	11	Екзамен
ОК6	Фізика	6	Екзамен
ОК7	Теорія ймовірності та математична статистика	4	Екзамен
ОК8	Комп'ютерна дискретна математика	4	Екзамен
ОК9	Алгоритми та структури даних	4	Екзамен
1.2. Обов'язкові компоненти професійної підготовки			
ОК10	Основи програмування	9	Екзамен
ОК11	Системи технічного захисту інформації	5	Екзамен
ОК12	Прикладна криптологія (+ курсова робота)	9	Екзамен
ОК13	Методи та засоби захисту інформації	6	Екзамен
ОК14	Математичні основи інформаційної безпеки	4	Екзамен
ОК15	Комп'ютерні мережі	5	Екзамен
ОК16	Локальні мережі	5	Екзамен
ОК17	Управління інформаційною безпекою	4	Екзамен
ОК18	Нормативно-правове та організаційне забезпечення систем захисту інформації	4	Залік
ОК19	Захист інформації в комп'ютерних мережах	5	Екзамен
ОК20	Комплексні системи захисту інформації (+ курсова робота)	5	Екзамен
ОК21	Теорія електричних та магнітних кіл	5	Екзамен
ОК22	Архітектура комп'ютерних	8	Екзамен

	систем		
ОК23	Вступ до спеціальності	3	Залік
ОК24	Комп'ютерна схемотехніка	6	Екзамен
ОК25	Арифметичні та логічні основи ЕОМ (+ курсовий проект)	7	Екзамен
ОК26	Бази даних	5	Екзамен
ОК27	Логічні основи штучного інтелекту	4	Екзамен
ОК28	Навчальна практика	4	Залік
ОК29	Навчально-технологічна практика	4	Залік
ОК30	Виробнича практика	4	Залік
ОК31	Дипломування	15	Захист роботи
2. Вибіркові компоненти (ВК)			
2.1. Вибіркові компоненти загальної підготовки			
ВК1.1	Філософія	4	Екзамен
ВК1.2	Проект людини в філософії		
ВК1.3	Філософська антропологія		
ВК2.1	Основи охорони праці	3	Екзамен
ВК2.2	Основи ергономіки на залізничному транспорті		
ВК2.3	Електробезпека та екологічна безпека		
ВК2.4	Цивільний захист		
ВК3.1	Основи екології та безпека життєдіяльності	4	Залік
ВК3.2	Основи загальної екології		
ВК3.3	Валеологія та безпека життєдіяльності		
ВК3.4	Екологія людини		
ВК4.1	Фізика (спеціальні розділи)	4	Екзамен
ВК4.2	Фізичні основи електротехніки		
ВК4.3	Комп'ютерна графіка		
ВК5.1	Фізичні основи бездротових мереж	4	Залік
ВК5.2	Теорія радіо кіл		
ВК5.3	Інженерна графіка		
ВК6.1	Теорія інформації та кодування	4	Залік
ВК6.2	Основи автоматизації контролю та управління на залізничному транспорті		
ВК6.3	Основи дискретної електроніки		
ВК7.1	Програмні засоби загального користування	4	Залік

ВК7.2	Програмування мовою Python		
ВК7.3	Об'єктно-орієнтоване програмування		
ВК8.1	Проектний практикум	4	Залік
ВК8.2	Візуальне програмування		
ВК8.3	Програмування мовою Delphi		
2.2. Вибіркові компоненти професійної підготовки			
ВК9.1	Комп'ютерна електроніка	4	Екзамен
ВК9.2	Комп'ютерна графіка		
ВК9.3	Інтелектуальні системи аналізу даних		
ВК10.1	ІНТЕРНЕТ технології	6	Залік
ВК10.2	Функціональна надійність та функціональна безпека схемотехнічних систем		
ВК10.3	Синтез мікропрограмних автоматів		
ВК11.1	Системне програмування	7	Екзамен
ВК11.2	Безпека програм та даних		
ВК11.3	Мова асемблера		
ВК12.1	Системне програмне забезпечення	7	Екзамен
ВК12.2	Теорія обчислювальних процесів і структур		
ВК12.3	Операційні системи		
ВК13.1	Проектування засобів захисту інформації на ПЛІС	4	Залік
ВК13.2	Побудова систем захисту залізничної автоматики		
ВК13.3	Схемотехніка функціонально захищених систем		
ВК14.1	Проектування мікропроцесорних систем захисту (+ курсова робота)	5	Залік
ВК14.2	Побудова мікропроцесорних систем захисту (+ курсова робота)		
ВК14.3	Програмування апаратних засобів захисту (+ курсова робота)		
ВК15.1	Мобільні пристрої та додатки	4	Залік
ВК15.2	Технології бездротових мереж		
ВК15.3	Сигнальні процесори		

Примітка*: дисципліна є позакредитною.

2.2. Розподіл змісту освітньо-професійної програми за групами компонентів та циклами підготовки

Цикл підготовки	**Обсяг навчального навантаження здобувача вищої освіти (кредитів / %)**		
	обов'язкові компоненти	**вибіркові компоненти**	**всього за весь термін навчання**
Цикл загальної підготовки	46/19	31/13	77/32
Цикл професійної підготовки	126/53	37/15	163/68
Всього за весь термін навчання	172/72	68/28	240/100

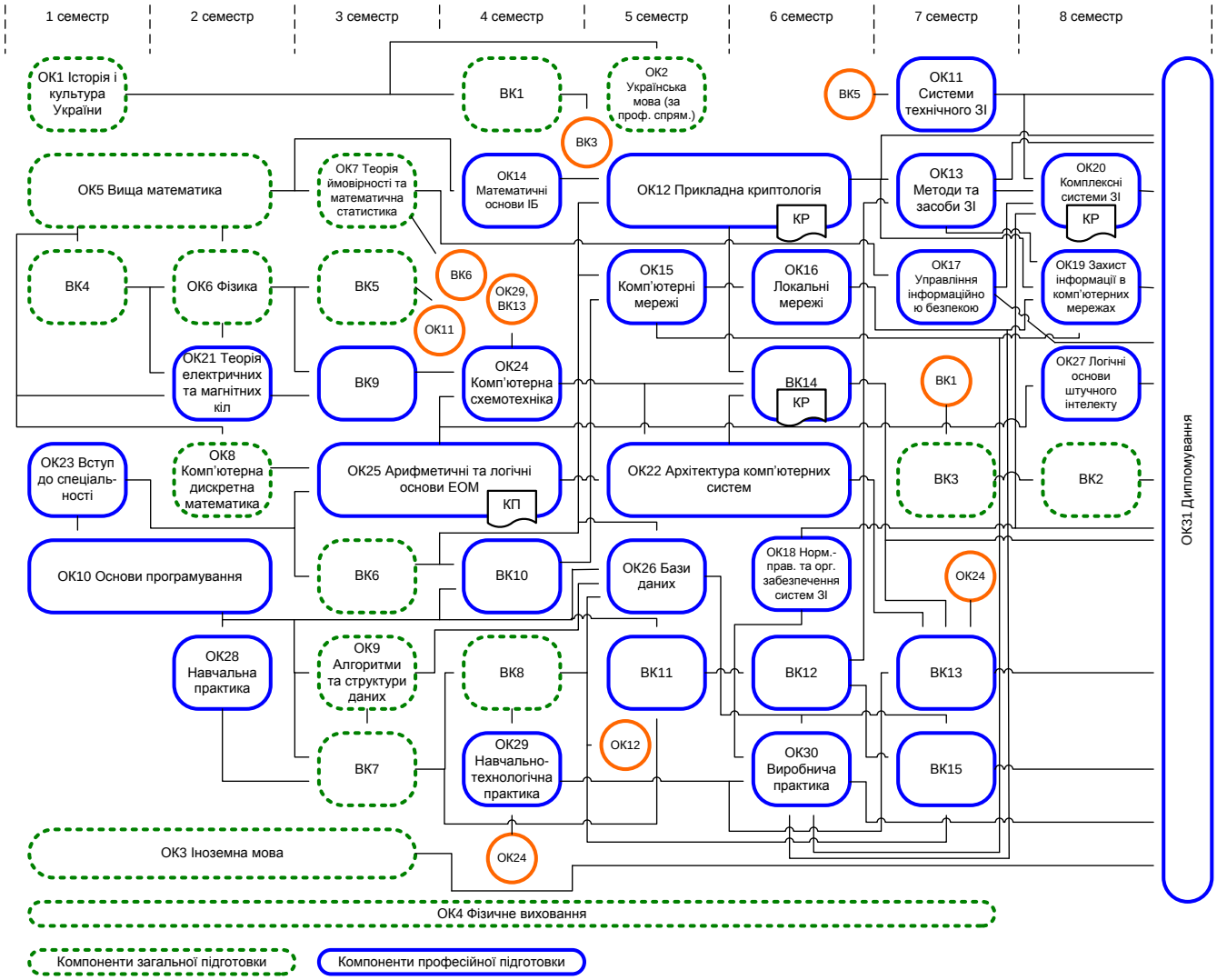
2.3. Структурно-логічна схема освітньої програми

Код навчальної дисципліни	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Код навчальної дисциплін, яка забезпечується зазначеною в стовпчику 1
1	2	
1. Обов'язкові компоненти (ОК)		
ОК1	Історія і культура України	ОК2
ОК2	Українська мова (за професійним спрямуванням)	ОК31
ОК3	Іноземна мова	ОК31
ОК4	Фізичне виховання	
ОК5	Вища математика	ОК6, ОК7, ОК8, ОК14, ОК21, ВК4
ОК6	Фізика	ОК21, ВК5, ВК9
ОК7	Теорія ймовірності та математична статистика	ОК17, ВК6
ОК8	Комп'ютерна дискретна математика	ОК25
ОК9	Алгоритми та структури даних	ОК26, ВК7
ОК10	Основи програмування	ОК28, ОК29, ВК7, ВК10, ВК11
ОК11	Системи технічного захисту інформації	ОК20, ОК31
ОК12	Прикладна криптологія (+ курсова робота)	ОК13, ОК19, ОК31
ОК13	Методи та засоби захисту інформації	ОК19, ОК20, ОК31
ОК14	Математичні основи інформаційної безпеки	ОК12

ОК15	Комп'ютерні мережі	ОК16, ОК19
ОК16	Локальні мережі	ОК19
ОК17	Управління інформаційною безпекою	ОК20, ОК31
ОК18	Нормативно-правове та організаційне забезпечення систем захисту інформації	ОК17, ОК20, ОК30, ОК31
ОК19	Захист інформації в комп'ютерних мережах	ОК31
ОК20	Комплексні системи захисту інформації (+ курсова робота)	ОК31
ОК21	Теорія електричних та магнітних кіл	ВК5, ВК9
ОК22	Архітектура комп'ютерних систем	ОК30, ВК13, ВК14
ОК23	Вступ до спеціальності	ОК10, ОК25, ВК6
ОК24	Комп'ютерна схемотехніка	ОК22, ОК29, ВК14
ОК25	Арифметичні та логічні основи ЕОМ (+ курсовий проект)	ОК22, ОК27
ОК26	Бази даних	ОК30, ВК15
ОК27	Логічні основи штучного інтелекту	ОК31
ОК28	Навчальна практика	ВК7
ОК29	Навчально-технологічна практика	ОК30, ВК13
ОК30	Виробнича практика	ОК31
ОК31	Дипломування	
2. Вибіркові компоненти (ВК)		
ВК1	Філософія	ВК3
	Проект людини в філософії	
	Філософська антропологія	
ВК2	Основи охорони праці	ОК31
	Основи ергономіки на залізничному транспорті	
	Електробезпека та екологічна безпека	
	Цивільний захист	
ВК3	Основи екології та безпека життєдіяльності	ВК2
	Основи загальної екології	
	Валеологія та безпека життєдіяльності	
	Екологія людини	
ВК4	Фізика (спеціальні розділи)	ОК6, ОК21

	Фізичні основи електротехніки	
	Комп’ютерна графіка	
ВК5	Фізичні основи бездротових мереж	ОК11
	Теорія радіо кіл	
	Інженерна графіка	
ВК6	Теорія інформації та кодування	ОК12, ОК13, ОК15, ОК26, ВК10
	Основи автоматизації контролю та управління на залізничному транспорті	
	Основи дискретної електроніки	
ВК7	Програмні засоби загального користування	ВК8, ВК11
	Програмування мовою Python	
	Об'єктно-орієнтоване програмування	
ВК8	Проектний практикум	ОК12, ОК29, ВК15
	Візуальне програмування	
	Програмування мовою Delphi	
ВК9	Комп’ютерна електроніка	ОК24
	Комп’ютерна графіка	
	Інтелектуальні системи аналізу даних	
ВК10	ІНТЕРНЕТ технології	ОК15
	Функціональна надійність та функціональна безпека схемотехнічних систем	
	Синтез мікропрограмних автоматів	
ВК11	Системне програмування	ВК12
	Безпека програм та даних	
	Мова асемблера	
ВК12	Системне програмне забезпечення	ОК13, ОК30, ВК15
	Теорія обчислювальних процесів і структур	
	Операційні системи	
ВК13	Проектування засобів захисту інформації на ПЛІС	ОК31
	Побудова систем захисту залізничної автоматики	
	Схемотехніка функціонально захищених систем	
ВК14	Проектування	ОК31, ВК13

	мікропроцесорних систем захисту (+ курсова робота)	
	Побудова мікропроцесорних систем захисту (+ курсова робота)	
	Програмування апаратних засобів захисту (+ курсова робота)	
ВК15	Мобільні пристрої та додатки	ОК31
	Технології бездротових мереж	
	Сигнальні процесори	



3. Форма атестації здобувачів вищої освіти

Атестація випускників за освітньою програмою «Кібербезпека» спеціальності 125 «Кібербезпека» проводиться у формі єдиного державного кваліфікаційного іспиту та (або) захисту кваліфікаційної роботи і завершується видачою документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації бакалавра з кібербезпеки.

Заклад вищої освіти забезпечує перевірку кваліфікаційної роботи на плагіат. Реферат кваліфікаційної роботи оприлюднюється у репозитарії університету. Захист кваліфікаційної роботи здійснюється відкрито та публічно.

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом спеціальності 125 «Кібербезпека» та цією освітньою програмою.

4. Матриця відповідності програмних компетентностей основним та вибірковим компонентам освітньої програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК8	ВК9	ВК10	ВК11	ВК12	ВК13	ВК14	ВК15
КЗ1			+	+	+	+	+													+								+	+	+						+										
КЗ2										+													+		+		+	+	+	+							+									
КЗ3		+	+																																											
КЗ4											+	+	+				+		+	+				+	+										+										
КЗ5				+		+	+	+	+	+				+		+		+			+	+	+			+	+	+			+		+	+	+	+	+	+			+			+
КЗ6	+																	+														+	+													
КЗ7	+	+		+	+	+	+	+													+										+	+	+	+	+	+								
КФ1																	+	+		+																									
КФ2									+	+		+	+		+	+	+		+									+									+	+	+		+				+
КФ3								+	+	+	+		+									+		+	+		+									+	+	+	+		+	+	+	+	+
КФ4																	+		+	+						+															+				
КФ5													+				+		+	+						+																+	+	+
КФ6															+	+								+					+	+												+	+			
КФ7											+		+				+	+		+																									
КФ8																	+					+																							
КФ9																	+												+	+															
КФ10											+	+	+	+					+	+																							+	+	
КФ11															+	+			+																								+			+
КФ12											+								+	+																									

5. Матриця відповідності програмних результатів навчання основним та вибірковим компонентам освітньої програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК8	ВК9	ВК10	ВК11	ВК12	ВК13	ВК14	ВК15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
ПР1	+	+	+																																											
ПР2																										+		+	+	+	+			+												
ПР3					+	+	+	+	+	+				+		+					+	+	+	+	+		+	+		+				+	+	+	+	+	+	+		+	+	
ПР4					+		+	+	+	+		+								+					+	+		+	+			+	+			+	+			+					
ПР5												+			+	+						+						+	+	+								+				+					+
ПР6					+	+	+	+									+	+	+					+		+		+						+	+				+						
ПР7																	+	+		+													+													
ПР8																	+	+		+																										
ПР9																	+	+													+															
ПР10											+		+		+	+			+	+		+		+	+		+				+						+					+		+			+
ПР11									+															+		+			+			+						+					+				+
ПР12																	+	+	+	+				+	+					+	+														
ПР13															+	+			+		+			+			+			+															
ПР14											+		+						+	+				+	+					+	+												+	+	+	+
ПР15										+	+								+	+																								+	+	+			
ПР16																			+	+										+																
ПР17													+			+		+				+	+	+			+																			
ПР18													+						+									+	+	+														+	+	

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
ПР19											+	+		+			+	+	+	+				+			+															+	+	+	
ПР20													+		+				+																											
ПР21													+				+	+		+						+																			
ПР22													+				+		+										+																
ПР23															+	+	+		+							+																+		+		
ПР24													+					+								+																		+			
ПР25													+						+							+																+				+
ПР26															+	+			+																									+			+
ПР27											+	+				+			+																								+				
ПР28																	+	+		+																											
ПР29																						+				+																				
ПР30											+								+	+						+																				
ПР31												+	+	+	+	+	+	+	+			+		+			+																+	+	+	+	+
ПР32																	+	+				+				+																+				
ПР33																	+		+			+																								
ПР34																	+	+				+	+							+																
ПР35																		+		+										+																
ПР36											+											+															+									
ПР37											+								+			+															+									
ПР38											+								+			+															+									
ПР39											+								+		+																								
ПР40											+								+		+																								

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
ПР41													+				+																														
ПР42																	+	+																													
ПР43																	+	+																													
ПР44							+										+	+																													
ПР45																	+													+																
ПР46																	+		+			+																								
ПР47												+	+						+																											
ПР48												+	+		+				+																											
ПР49													+				+		+					+																					
ПР50																	+								+																		+			+
ПР51															+		+		+						+																					+
ПР52																	+		+			+				+			+	+												+	+			
ПР53										+				+			+		+									+		+	+		+						+	+	+		+	+	+	+	+	+
ПР54	+	+	+																													+	+	+													