


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
КАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ІМЕНІ ВАСИЛЯ СТЕФАНІКА  
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ  
«ІВАНО-ФРАНКІВСЬКИЙ ФАХОВИЙ КОЛЕДЖ КАРПАТСЬКОГО  
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ  
ІМЕНІ ВАСИЛЯ СТЕФАНІКА»

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА**  
**«КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»**

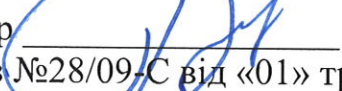
освітньо-професійного ступеня “Фаховий молодший бакалавр”  
за спеціальністю F5 Кібербезпека та захист інформації  
галузі знань F Інформаційні технології

Освітня кваліфікація: **Фаховий молодший бакалавр**  
**з кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО ПЕДАГОГІЧНОЮ РАДОЮ**

Голова ради  **Юрій МОСКАЛЕНКО**  
(протокол № 03 від «30» квітня 2026 року)

Освітньо-професійна програма вводиться в дію  
з «01» вересня 2026 року

Ректор  **Валентина ЯКУБІВ**  
(наказ №28/09-С від «01» травня 2026 року)

**м. Івано-Франківськ**  
**2026 рік**

## ЛИСТ-ПОГОДЖЕННЯ

освітньо-професійної програми  
фахова передвища освіта


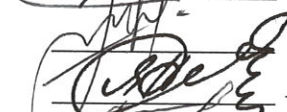
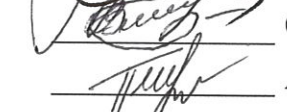

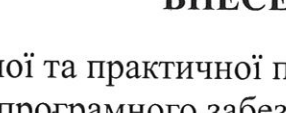
### ЗАПРОПОНОВАНО

#### Робоча група:

Голова робочої групи

(Гарант)

Члени робочої групи

 Андрій АНИЧ  
 Тарас БЕДРІЙ  
 Ярослав НИКОРАК  
 Ольга ГАНДЕРА-КАЛИНОВСЬКА  
 Анна ПАВЛИШАК

### ВНЕСЕНО:

Циклова комісія професійної та практичної підготовки  
(спеціальність «Інженерія програмного забезпечення»)  
Протокол № 09 від 23 березня 2026 року

Голова циклової комісії  Тарас БЕДРІЙ

### ПОГОДЖЕНО:

Педагогічною радою Відокремленого структурного  
підрозділу «Івано-Франківський фаховий коледж Карпатського  
національного університету імені Василя Стефаника».  
Протокол №03 від «30» квітня 2026 року.

Голова Педагогічної ради  Юрій МОСКАЛЕНКО

### НАДАНО ЧИННОСТІ

Наказ ректора № 28/09-С від «01 » травня 2026 року

### ВВЕДЕНО В ДІЮ З:

«01» вересня 2026 року

Навчально-методичний відділ

Начальник  Ірина СОЛОНЕЦЬ

## ПЕРЕДМОВА

Освітньо-професійна програма є нормативним документом, який регламентує нормативні компетентнісні, кваліфікаційні, організаційні, навчальні та методичні вимоги у підготовці здобувачів рівня фахової передвищої освіти ступеня фахового молодшого бакалавра галузі F Інформаційні технології спеціальності F5 Кібербезпека та захист інформації, заснована на компетентнісному підході підготовки фахівців у галузі F Інформаційні технології спеціальності F5 Кібербезпека та захист інформації.

Освітньо-професійна програма розроблена на виконання вимог Закону України «Про фахову передвищу освіту» від 06.06.2019 року №2745-VIII, Національної рамки кваліфікацій (постанова Кабінету Міністрів України від 23.11.2011 року №1341, із змінами, внесеними постановою Кабінету Міністрів України від 05.02.2026 року №159), наказу Міністерства освіти і науки України від 19.11.2024 року №1625 «Про особливості запровадження змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затверджених постановою Кабінету Міністрів України від 30.08.2024 року №1021», відповідно до вимог Положення про освітньо-професійні програми у Відокремленому структурному підрозділі «Івано-Франківський фаховий коледж Карпатського національного університету імені Василя Стефаника», введеного в дію наказом в.р. ректора наказом в. о. ректора Карпатського національного університету імені Василя Стефаника від 22 вересня 2025 р. № 843.

Освітньо-професійна програма розглянута та затверджена Педагогічною радою Івано-Франківського фахового коледжу Карпатського національного університету імені Василя Стефаника» від «30» квітня 2026 року протокол №03; надано чинності наказом ректора №28/09-С від «01» травня 2026 року.

Освітньо-професійна програма вводиться в дію з 01.09.2026 року.

### **Розроблено робочою групою у складі:**

Аннич Андрій Богданович – спеціаліст вищої категорії, викладач Відокремленого структурного підрозділу «Івано-Франківський фаховий коледж Карпатського національного університету імені Василя Стефаника», голова робочої групи, гарант.

Бедрій Тарас Романович – спеціаліст вищої категорії, викладач-методист, завідувач відділення інформаційних технологій Відокремленого структурного підрозділу «Івано-Франківський фаховий коледж Карпатського національного університету імені Василя Стефаника».

Никорак Ярослав Ярославович - спеціаліст вищої категорії, викладач-методист, заступник директора з навчально-методичної роботи Відокремленого структурного підрозділу «Івано-Франківський фаховий коледж Карпатського національного університету імені Василя Стефаника».

Гандера-Калиновська Ольга Володимирівна – спеціаліст першої категорії, викладач Відокремленого структурного підрозділу «Івано-Франківський фаховий коледж Карпатського національного університету імені Василя Стефаника».

Павлишак Анна Юріївна – здобувач фахової передвищої освіти за спеціальністю 113 Прикладна математика Відокремленого структурного підрозділу «Івано-Франківський фаховий коледж Карпатського національного університету імені Василя Стефаника».

**Профіль освітньо-професійної програми  
зі спеціальності F5 «Кібербезпека та захист інформації»**

<b>1. Загальна інформація</b>	
<i>Повна назва закладу фахової передвищої освіти</i>	Відокремлений структурний підрозділ «Івано-Франківський фаховий коледж Карпатського національного університету імені Василя Стефаника»
<i>Рівень освіти</i>	Фахова передвища освіта
<i>Освітньо-професійний ступінь</i>	Фаховий молодший бакалавр
<i>Галузь знань</i>	F Інформаційні технології
<i>Спеціальність</i>	F5 Кібербезпека та захист інформації
<i>Офіційна назва освітньо-професійної програми</i>	Кібербезпека та захист інформації
<i>Форма здобуття освіти</i>	Інституційна (очна(денна))
<i>Тип диплома та обсяг освітньо-професійної програми</i>	Диплом фахового молодшого бакалавра, одиничний, 180 кредитів ECTS, термін навчання – 3 роки і 10 місяців
<i>Освітня кваліфікація</i>	Фаховий молодший бакалавр з кібербезпеки та захисту інформації
<i>Професійна кваліфікація</i>	Не надається
<i>Кваліфікація в дипломі</i>	Освітньо-професійний ступінь - фаховий молодший бакалавр Спеціальність - F5 Кібербезпека та захист інформації Освітньо-професійна програма - Кібербезпека та захист інформації
<i>Наявність акредитації</i>	Вперше
<i>Цикл/рівень</i>	Рівень фахової передвищої освіти, 5 рівень НРК України -
<i>Передумови</i>	На основі базової середньої, з одночасним здобуттям профільної середньої освіти. Наявність повної загальної середньої освіти
<i>Мова(и) викладання</i>	Українська

<i>Термін дії освітньої програми</i>	5 років
<i>Інтернет-адреса постійного розміщення опису освітньо-професійної програми</i>	<a href="https://ifk.cnu.edu.ua/osvitno-profesijnyj-stupin-fakhovo/">https://ifk.cnu.edu.ua/osvitno-profesijnyj-stupin-fakhovo/</a>
<p><b>2. Мета освітньо-професійної програми</b></p> <p>Підготовка компетентних конкурентоспроможних фахівців у сфері інформаційної та/або кібербезпеки, здатних успішно вирішувати типові спеціалізовані задачі та практичні проблеми, пов'язані із використанням сучасного програмного та програмно-апаратного забезпечення (засобів) кіберзахисту</p>	
<p><b>3. Характеристика освітньої програми</b></p>	
<i>Предметна область (галузь знань, спеціальність)</i>	<p>Галузь знань – Інформаційні технології          Спеціальність – Кібербезпека та захист інформації  <b>Об'єкти вивчення:</b> технології кібербезпеки та захисту інформації; процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології.  <b>Цілі навчання:</b> підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації.  <b>Теоретичний зміст предметної області:</b> Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору; своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.  <b>Методи, методики та технології:</b> методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації;  <b>Інструменти та обладнання:</b> засоби, пристрої, мережеве устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).</p>

<p><b>Орієнтація освітньо-професійної програми</b></p>	<p>Освітньо-професійна програма (фахового молодшого бакалавра)          Прикладна орієнтація          Освітньо-професійна програма базується на загальнонаукових та практичних результатах в кібербезпеці і має прикладну орієнтацію напрямку інтеграції програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності.          Освітні компоненти ОПП спрямовані на вивчення актуальних тем з метою професійного становлення здобувача фахової передвищої освіти.</p>
<p><b>Основний фокус освітньо-професійної програми та спеціалізації</b></p>	<p>Акцент на знаннях в області систематизованого й упорядкованого підходу до забезпечення кібербезпеки, захисту інформації та реагування на інциденти на основі використання принципів інформаційної безпеки стосовно процесів оцінки загроз і впровадження захисних заходів, а також здатність їхнього застосування в практичній діяльності.          Ключові слова: кібербезпека, захист інформації, аналіз загроз, криптографія, аудит безпеки.</p>
<p><b>Особливості освітньо-професійної програми</b></p>	<p>Освітньо-професійна програма спрямована на підготовку висококваліфікованих здобувачів освіти освітньо-професійного ступеня фаховий молодший бакалавр з кібербезпеки та захисту інформації шляхом здобуття фундаментальних, теоретико-методичних, фахових знань, практичних умінь, навичок та інших компетентностей, достатніх для розв'язування типових спеціалізованих задач у професійній діяльності.          Унікальність освітньо-професійної програми полягає у використанні сучасних технологій кібербезпеки з акцентом на системах Internet of Things, хмарних сервісах, Big Data (аналіз загроз), супроводі систем захисту та безпеки загального та спеціального призначення, створенні та впровадженні інтелектуальних рішень для виявлення та реагування на кіберінциденти.</p>
<p><b>4. Придатність випускників до працевлаштування та подальшого навчання</b></p>	

<b>Придатність до працевлаштування</b>	<p>Фаховий молодший бакалавр за спеціальністю F5 Кібербезпека та захист інформації здатний ефективно розв'язувати типові професійні завдання й практичні проблеми у сфері кібербезпеки та захисту інформації, а також виконувати професійну діяльність відповідно до Національного класифікатора професій ДК 003:2010 (зі змінами), обіймаючи первинні посади:</p> <ul style="list-style-type: none"> <li>-3119 - технік (сфера захисту інформації);</li> <li>- 3439 - фахівець із організації інформаційної безпеки;</li> <li>- 3439 - фахівець із організації захисту інформації з обмеженим доступом;</li> <li>- 3439 - фахівець з режиму секретності;</li> <li>-3121 - фахівець з інформаційних технологій.</li> </ul>
<b>Подальше навчання</b>	<p>Здобуття освіти за: початковим рівнем (короткий цикл) вищої освіти; першим (бакалаврський) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.</p>
<b>5. Викладання та оцінювання</b>	
<b>Викладання та навчання</b>	<p><b>Методи</b> – проблемно-пошукові, діалогічні, дослідницькі, евристичні, інтерактивні (вебінари, тренінги, презентації, дистанційні освітні ресурси та цифрові технології). Методи навчання конкретизовані на рівні всіх освітніх компонентів у силабусах, робочих навчальних програмах.</p> <p><b>Підходи</b> – академічний підхід; студентоцентристський підхід.</p> <p><b>Технології</b> – активного навчання (проблемні, інтерактивні, проєктні, інформаційно-комп'ютерні, саморозвивальні, технологія співпраці).</p> <p>Студентоцентроване навчання, проблемно-орієнтоване викладання, самонавчання, електронного навчання в системі D-learn, навчання на основі проведення навчальної та виробничої практики тощо.</p> <p>Викладання здійснюється у формі мультимедійних та інтерактивних лекцій, семінарів, практичних занять, самостійного навчання, індивідуальних занять тощо.</p> <p>Для досягнення програмних результатів використовуються такі освітні технології: активно-продуктивні (проблемні, імітаційні, дискусійні, проєктні, інформаційно-комунікаційні, контекстного навчання, співробітництва); електронні навчальні курси, мережі Internet. Навчання здійснюється з використанням платформ Google Meet, Google Classroom, Zoom.</p>

<b>Оцінювання</b>	<p>Система оцінювання будується на умовах академічної доброчесності та прозорості за 100-бальною шкалою з переведенням у систему оцінок за національною шкалою, а також забезпечення ранжування досягнень за шкалою ECTS. З урахуванням результатів неформальної та інформальної освіти.</p> <p><b>Види контролю:</b> поточний, тематичний, підсумковий, самоконтроль.</p> <p><b>Форми контролю:</b> усне та письмове опитування, тестування, презентації, заліки, екзамени, захист курсових робіт, звітів з практики, підсумкова атестація у формі захисту кваліфікаційної роботи.</p>
<b>6. Перелік компетентностей випускника</b>	
<b>Інтегральна компетентність</b>	<p>Здатність вирішувати типові спеціалізовані задачі в галузі кібербезпеки або у процесі навчання, що вимагає застосування положень і методів відповідних наук та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності; здійснювати контроль інших осіб у визначених ситуаціях.</p>
<b>Загальні компетентності (ЗК)</b>	<p><b>ЗК1.</b> Здатність застосовувати знання у різних практичних ситуаціях.</p> <p><b>ЗК2.</b> Знання та розуміння предметної області та розуміння професії.</p> <p><b>ЗК3.</b> Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.</p> <p><b>ЗК4.</b> Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p><b>ЗК5.</b> Здатність до пошуку, оброблення та аналізу інформації.</p> <p><b>ЗК6.</b> Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p><b>ЗК7.</b> 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.</p>

**Спеціальні (фахові)  
компетентності**

- СК1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, рекомендовані практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки.
- СК2.** Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей кібербезпеки.
- СК3.** Здатність до розробки та використання програмних та програмно-апаратних засобів захисту інформації для забезпечення кібербезпеки.
- СК4.** Здатність забезпечувати працездатність інформаційно-комунікаційних систем згідно з встановленою політикою кібербезпеки.
- СК5.** Здатність забезпечувати захист інформації для реалізації встановленої політики кібербезпеки установи чи підприємства.
- СК6.** Здатність відновлювати штатне функціонування інформаційно-комунікаційних систем після реалізації кіберзагроз, збоїв і відмов різних класів та походження.
- СК7.** Здатність забезпечувати функціонування комплексних систем захисту інформації.
- СК8.** Здатність здійснювати протидію несанкціонованому проникненню в інформаційно-комунікаційні системи і мережі.
- СК9.** Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
- СК10.** Здатність застосовувати методи та засоби криптографічного, стенографічного і технічного захисту інформації.
- СК11.** Здатність виконувати моніторинг процесів функціонування та тестування інформаційно-комунікаційних систем згідно з встановленою політикою кібербезпеки.
- СК12.** Здатність застосовувати теоретичні знання та практичні навички з організації та функціонування сучасних операційних систем, уміння зі створення та використання безпечного програмного забезпечення для керування обчислювальними ресурсами в багатокористувацьких операційних системах.
- СК13.** Здатність виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційного простору та інформаційних ресурсів згідно з встановленою політикою інформаційної та/або кібербезпеки.
- СК14.** Здатність до вибору захищених хмарних платформ та сервісів, безпечного розгортання на них, інтегрування, адміністрування і супроводу інформаційних систем.

**7. Нормативний зміст підготовки здобувачів фахової передвищої освіти,  
сформульований у термінах результатів навчання**

**РН1.** Знати законодавчу та нормативно-правову базу України та вимоги відповідних стандартів, у тому числі міжнародних, в галузі інформаційної безпеки та/або кібербезпеки.

- PH2.** Знати національні та міжнародні стандарти, регулюючі акти виявлення, ідентифікації, аналізу та реагування на інциденти в сфері інформаційної безпеки та/або кібербезпеки.
- PH3.** Знати державну та іноземні мови з метою забезпечення ефективності професійної комунікації.
- PH4.** Вміти адаптуватися до умов частотої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
- PH5.** Вміти використовувати сучасні програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
- PH6.** Вміти використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного вирішення спеціалізованих задач професійної діяльності.
- PH7.** Знати основні методи розробки моделі загроз та порушника.
- PH8.** Вміти використовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
- PH9.** Знати теорію та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
- PH10.** Вміти забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
- PH11.** Вміти впроваджувати заходи щодо попередження отримання несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем згідно зі встановленою політикою інформаційної безпеки та/або кібербезпеки.
- PH12.** Вміти вирішувати задачі щодо управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
- PH13.** Вміти вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах, в тому числі з використанням сучасних методів та засобів криптографічного захисту інформації.
- PH14.** Вміти вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
- PH15.** Вміти 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.
- PH16.** Знати системи виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
- PH17.** Вміти підтримувати працездатність з використанням інструментарію для моніторингу процесів в інформаційно-телекомунікаційних системах.
- PH18.** Вміти вирішувати задачі аналізу програмного коду на наявність можливих загроз.
- PH19.** Вміти вирішувати задачі безпеки функціонування інформаційних систем, розгорнутих на хмарних платформах.

## 8. Ресурсне забезпечення реалізації програми

### *Кадрове забезпечення*

Для реалізації освітньо-професійної програми залучений педагогічний склад, який за кваліфікацією відповідає профілю і напряму дисциплін, що викладаються, має необхідний стаж педагогічної та практичної роботи відповідно до Ліцензійних умов провадження освітньої діяльності затверджених Постановою Кабінету Міністрів України від 30.12.2015 року №1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності (в редакції постанов Кабінету Міністрів України від 24.03.2021 року №365, від 31.10.2023 року №1134), Положення про кадрове забезпечення освітнього процесу, кадрове забезпечення освітньо-професійних програм у відокремленому структурному підрозділі Івано-Франківський фаховий коледж Карпатського національного університету імені Василя Стефаника» (введено в дію наказом ректора Карпатського національного університету імені Василя Стефаника від 09 березня 2026 р. № 317).

Усі викладачі періодично за планом проходять курси підвищення кваліфікації, стажування, беруть участь у проєктах, тренінгах, онлайн-курсах.

### *Матеріально-технічне забезпечення*

Матеріально-технічне забезпечення освітньої програми відповідає чинним вимогам до проведення освітньої діяльності у сфері вищої освіти: навчальні приміщення відповідають санітарним нормам та вимогам правил пожежної безпеки; забезпечення освітнього процесу мультимедійною технікою. Для проведення інформаційного пошуку є спеціалізований комп'ютерний кабінет, де наявний необмежений відкритий доступ до Інтернет-мережі. Наявна вся необхідна соціально-побутова інфраструктура, кількість місць у гуртожитку відповідає вимогам.

<p><b>Інформаційне та навчально-методичне забезпечення</b></p>	<ul style="list-style-type: none"> <li>- офіційний веб-сайт містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти;</li> <li>- доступ до мережі Інтернет (в тому числі і в гуртожитку);</li> <li>- бібліотека з необхідною кількістю фахових видань, читальна зала;</li> <li>- навчальні й робочі навчальні плани, робочі програми, силабуси;</li> <li>- графіки навчального процесу ;</li> <li>- навчально-методичні комплекси забезпечення дисциплін;</li> <li>- дидактичні матеріали для самостійної та індивідуальної роботи студентів з дисциплін, наскрізні програми практик;</li> <li>- методичні вказівки щодо виконання курсових проєктів, методичне забезпечення державної атестації студентів; програм практик; методичних вказівок щодо виконання курсових робіт.</li> </ul>
<p><b>9. Академічна мобільність</b></p>	
<p><b>Національна мобільність</b>                      <b>кредитна</b></p>	<p>Організація академічної мобільності освітнього процесу за спеціальністю регламентується Положенням про академічну мобільність учасників освітнього процесу Карпатського національного університету імені Василя Стефаника <a href="http://nmv.pnu.edu.ua/wp-content/uploads/sites/118/2018/04/Polozhennia-pro-akademichnu-mobilnist-uchasnykiv-osvitnoho-protse-su.pdf">http://nmv.pnu.edu.ua/wp-content/uploads/sites/118/2018/04/Polozhennia-pro-akademichnu-mobilnist-uchasnykiv-osvitnoho-protse-su.pdf</a>.</p>
<p><b>Навчання здобувачів освіти</b>                      <b>іноземних</b></p>	<p>Не передбачено</p>

## 2. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

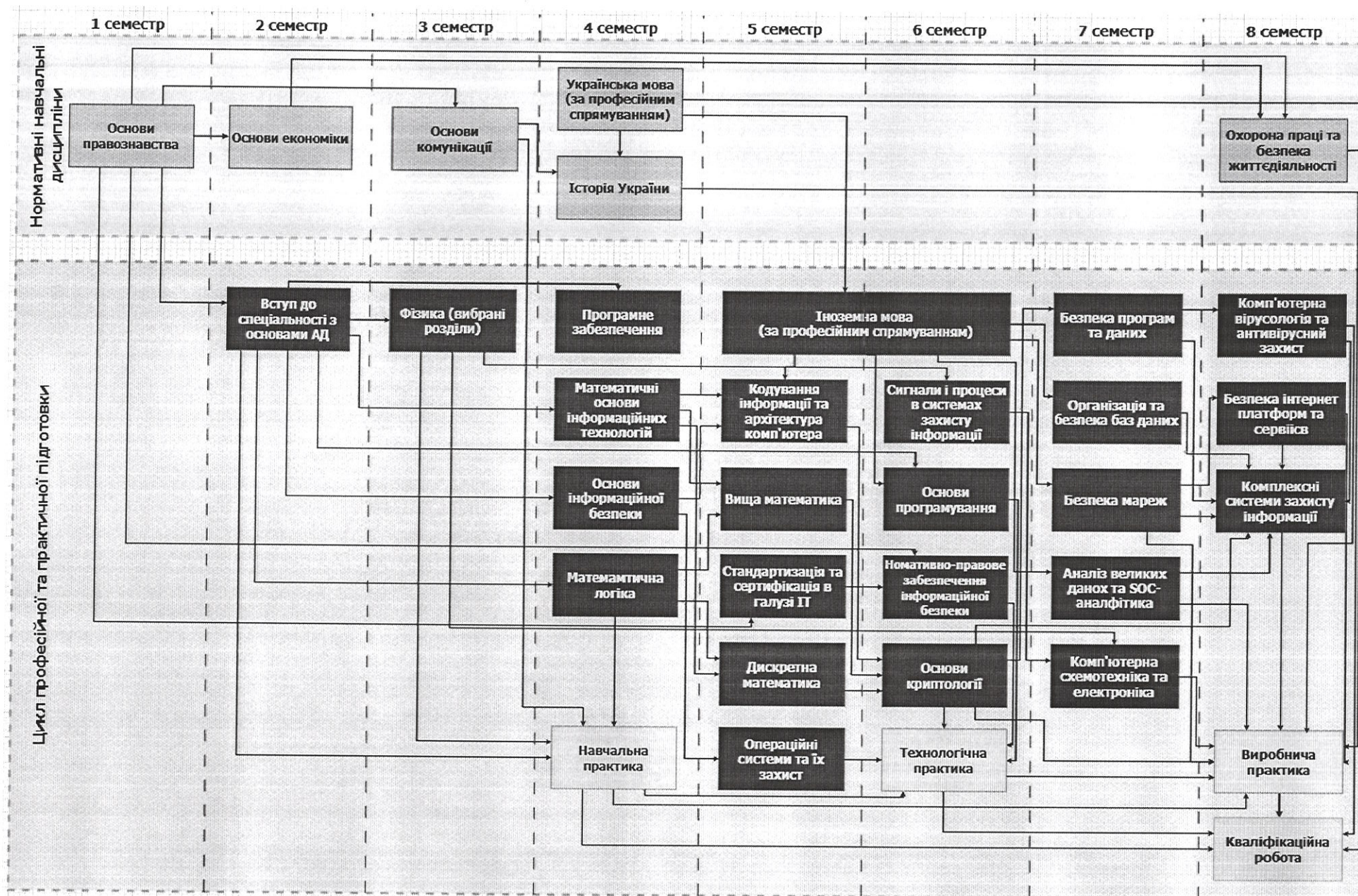
### 2.1 Перелік компонентів освітньо-професійної програми

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Семестр	Форма підсумкового контролю
<b>Обов'язкові компоненти ОПП</b>				
<b>2. Нормативні освітні компоненти</b>				
<b>2.1. Цикл загальної підготовки</b>				
<b>ОК 1</b>	Українська мова (за професійним спрямуванням)(Українська мова)	3	4	екзамен
<b>ОК 2</b>	Основи комунікації	3	3	залік
<b>ОК 3</b>	Іноземна мова (за професійним спрямуванням)	9	5,6	екзамен
<b>ОК 4</b>	Охорона праці та безпека життєдіяльності	3	8	залік
<b>ОК 5</b>	Вступ до спеціальності з основами академічної доброчесності (Технології)	3	2	залік
<b>ОК 6</b>	Історія України	3	4	залік
<b>ОК 7</b>	Основи правознавства (Громадянська освіта)	3	1	залік
<b>ОК 8</b>	Основи економічної теорії (Громадянська освіта)	3	2	залік
<b>Всього за циклом загальної підготовки</b>		<b>30,0</b>		
<b>2.2. Цикл професійної підготовки</b>				
<b>2.2.1. Теоретична підготовка</b>				
<b>ОК9</b>	Основи інформаційної безпеки	3	4	залік
<b>ОК10</b>	Кодування інформації та архітектура комп'ютерів	6	5	залік курсний проєкт
<b>ОК 11</b>	Безпека програм та даних	3	7	залік

<b>ОК 12</b>	Сигнали і процеси в системах захисту інформації	6	6	залік
<b>ОК 13</b>	Організація та безпека баз даних	6	7	екзамен курсний проєкт
<b>ОК 14</b>	Нормативно-правове забезпечення інформаційної безпеки	3	6	залік
<b>ОК 15</b>	Вища математика	6	5	екзамен
<b>ОК 16</b>	Комп'ютерні мережі	6	7	екзамен
<b>ОК 17</b>	Основи програмування	6	6	екзамен
<b>ОК 18</b>	Основи криптології	6	6	екзамен курсний проєкт
<b>ОК 19</b>	Стандартизація та сертифікація в галузі ІТ	3	5	залік
<b>ОК 20</b>	Комп'ютерна вірусологія та антивірусний захист	6	8	екзамен
<b>ОК 21</b>	Безпека мереж	3	7	залік
<b>ОК 22</b>	Безпека інтернет платформ та сервісів	6	8	екзамен
<b>ОК 23</b>	Аналіз великих даних та SOC-аналітика	6	7	екзамен
<b>ОК 24</b>	Операційні системи та їх захист	6	5	екзамен
<b>ОК 25</b>	Комплексні системи захисту інформації	3	8	залік
<b>ОК 26</b>	Комп'ютерна схемотехніка та електроніка	3	7	залік
<b>ОК 27</b>	Фізика (вибрані розділи)	3	3	залік
<b>ОК 28</b>	Програмне забезпечення	3	4	залік
<b>ОК 29</b>	Математичні основи інформаційних технологій	3	4	залік
<b>ОК 30</b>	Дискретна математика	6	5	екзамен
<b>ОК 31</b>	Математична логіка	3	4	екзамен

<i>Всього за пунктом 2.2.1</i>		<i>105,0</i>		
<b>2.2.2.Практична підготовка</b>				
<b>ОК 32</b>	Навчальна практика	3	4	залік
<b>ОК 33</b>	Технологічна практика	9	6	залік
<b>ОК 34</b>	Виробнича практика	12	8	залік
<i>Всього за пунктом 2.2.2</i>		<i>24,0</i>		
<i>Всього за циклом професійної підготовки</i>		<i>129,0</i>		
<i>Загальний обсяг обов'язкових компонент</i>		<i>159,0</i>		
<b>3. Вибіркові компоненти</b>				
<b>ВК 1</b>	Вибіркова компонента ОПП 1	3	5	залік
<b>ВК 2</b>	Вибіркова компонента ОПП 2	3	5	залік
<b>ВК 3</b>	Вибіркова компонента ОПП 3	3	6	залік
<b>ВК 4</b>	Вибіркова компонента ОПП 4	3	6	залік
<b>ВК 5</b>	Вибіркова компонента ОПП 5	3	7	залік
<b>ВК 6</b>	Вибіркова компонента ОПП 6	3	7	залік
<i>Загальний обсяг вибірових компонент</i>		<i>18,0</i>		
<b>4. Атестація</b>				
<b>ОК 35</b>	Кваліфікаційна робота	3	8	захист кваліфікаційної роботи
<i>Всього</i>		<i>3,0</i>		
<b>Загальний обсяг освітньо-професійної програми</b>		<b>180,0</b>		

## 2.2 Структурно-логічна схема



### 3. Форма атестації здобувачів освіти

<b>Форми атестації здобувачів фахової передвищої освіти</b>	Атестація здобувачів фахової передвищої освіти здійснюється у формі кваліфікаційної роботи.
<b>Вимоги до кваліфікаційної роботи</b>	Кваліфікаційна робота має передбачати розв'язання типової задачі кібербезпеки та захисту інформації, що характеризується комплексністю та/або невизначеністю умов. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації.

Атестація випускників здійснюється відкрито і публічно і проводиться у формі публічного захисту (демонстрації) кваліфікаційної роботи та завершується видачею документа встановленого зразка про присудження освітньо-професійного ступеня фахового молодшого бакалавра із присвоєнням кваліфікації фаховий молодший бакалавр з кібербезпеки та захисту інформації».

#### Вимоги до професійних стандартів

Не передбачено

Гарант освітньо-професійної програми



Андрій АННИЧ

**Матриця відповідності визначених Стандартом компетентностей/ результатів навчання дескрипторам  
Національної рамки кваліфікацій**

<b>Класифікація компетентностей за НРК</b>	<b>Знання</b>	<b>Уміння/ навички</b>	<b>Комунікація</b>	<b>Відповідальність і автономія</b>
	<p><b>Зн1.</b> Всебічні спеціалізовані теоретичні знання у сфері професійної діяльності та/або навчання, усвідомлення меж цих знань.</p> <p><b>Зн2.</b> Всебічні спеціалізовані емпіричні знання у сфері професійної діяльності та/або навчання, усвідомлення меж цих знань.</p>	<p><b>Ум1.</b> Широкий спектр когнітивних та практичних умінь /навичок, необхідних для розв'язання складних задач у спеціалізованих сферах професійної діяльності та/ або навчання; знаходження творчих рішень або відповідей на чітко визначені конкретні та абстрактні проблеми на основі ідентифікації та застосування даних; планування, аналіз, контроль та оцінювання власної роботи та роботи інших осіб у спеціалізованому контексті.</p>	<p><b>К1.</b> Взаємодія з колегами, керівниками та клієнтами у питаннях, що стосуються розуміння, навичок та діяльності у професійній сфері та/ або у сфері навчання</p> <p><b>К2.</b> Донесення до широкого кола осіб (колеги, керівники, клієнти) власного розуміння, знань, суджень, досвіду, зокрема у сфері професійної діяльності.</p>	<p><b>АВ1.</b> Організація та нагляд (управління) в контекстах професійної діяльності або навчання в умовах непередбачуваних змін; покращення результатів власної діяльності і роботи інших.</p> <p><b>АВ2.</b> Здатність продовжувати навчання з деяким ступенем автономії</p>
<b>Загальні компетентності (ЗК)</b>				
<b>ЗК01</b>	<b>Зн1</b>	<b>Ум1</b>	<b>К1, К2</b>	<b>ВА2</b>
<b>ЗК02</b>	<b>Зн1</b>		<b>К1, К2</b>	<b>ВА2</b>
<b>ЗК03</b>	<b>Зн1</b>		<b>К1, К2</b>	<b>ВА2</b>
<b>ЗК04</b>	<b>Зн1</b>		<b>К1, К2</b>	<b>ВА2</b>
<b>ЗК05</b>	<b>Зн1</b>	<b>Ум1</b>		<b>ВА2</b>
<b>ЗК06</b>	<b>Зн1</b>	<b>Ум2</b>		<b>ВА2</b>
<b>ЗК07</b>	<b>Зн1</b>	<b>Ум1</b>		<b>ВА3</b>

**Спеціальні (фахові, предметні) компетентності (СК)**

СК01	Зн1	Ум1		
СК02	Зн1	Ум1	К1, К2	БА2, БА3
СК03	Зн1	Ум1		БА1, БА2, БА3
СК04	Зн1	Ум1, Ум3	К1, К2	БА1, БА3
СК05	Зн1	Ум1, Ум2	К1, К2	БА2, БА3
СК06	Зн1	Ум1, Ум2	К1, К2	БА1, БА2, БА3
СК07	Зн1	Ум1, Ум2	К1, К2	БА1, БА2, БА3
СК08	Зн1	Ум1, Ум3	К1, К2	БА1, БА2, БА3
СК09	Зн1	Ум1, Ум3	К1, К2	БА1, БА2, БА3
СК10	Зн1	Ум1, Ум2, Ум3	К2	БА1, БА2, БА3
СК11	Зн1	Ум2, Ум3	К2	БА2, БА3
СК12	Зн1	Ум1, Ум2, Ум3	К2	БА2, БА3
СК13	Зн1	Ум1, Ум3	К1	БА3
СК14	Зн1	Ум1, Ум3	К1	БА1, БА2, БА3

#### 4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35			
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		
ЗК1	+		+	+				+					+								+				+	+						+	+	+	+			
ЗК2				+	+				+	+	+	+	+			+		+				+	+	+	+	+							+	+	+	+		
ЗК3	+	+	+																																		+	
ЗК4									+					+				+						+													+	
ЗК5		+							+	+			+		+			+						+					+		+	+	+				+	
ЗК6		+				+	+	+					+																								+	
ЗК7						+	+	+																													+	
СК1							+						+					+																			+	
СК2											+					+					+	+	+												+	+	+	
СК3										+	+	+					+				+	+	+		+		+									+	+	+
СК4											+		+			+					+	+		+	+		+				+	+	+	+	+	+	+	
СК5									+		+		+				+			+	+	+			+												+	
СК6													+			+									+	+			+						+	+	+	
СК7									+																+												+	
СК8									+				+			+					+		+			+											+	
СК9		+							+					+										+			+										+	
СК10										+		+			+		+									+		+	+	+	+	+	+	+	+		+	
СК11									+			+								+				+	+					+				+	+	+		
СК12																					+		+		+				+						+	+	+	
СК13									+													+			+		+										+	
СК14											+											+	+												+	+	+	

Гарант освітньо-професійної програми

 Андрій АНИЧ

## Матриця забезпечення програмних результатів навчання відповідними компонентами освітньо-професійної програми

	OK 1	OK 2	OK 3	OK 4	OK 5	OK 6	OK 7	OK 8	OK 9	OK 10	OK 11	OK 12	OK 13	OK 14	OK 15	OK 16	OK 17	OK 18	OK 19	OK 20	OK 21	OK 22	OK 23	OK 24	OK 25	OK 26	OK 27	OK 28	OK 29	OK 30	OK 31	OK 32	OK 33	OK 34	OK 35
PH 1						+	+						+						+																+
PH 2							+		+										+				+												+
PH 3	+	+	+																																+
PH 4					+				+				+		+					+		+	+	+				+			+			+	
PH 5													+							+				+	+			+					+	+	+
PH 6					+	+								+									+					+					+	+	+
PH 7					+				+			+	+					+					+	+				+	+			+		+	+
PH 8											+					+					+	+		+	+			+				+		+	
PH 9					+				+	+		+					+	+												+	+	+		+	
PH 10									+				+							+		+		+				+					+	+	+
PH 11				+							+					+					+	+		+	+	+		+				+	+	+	
PH 12											+		+			+					+	+		+	+	+		+				+	+	+	
PH 13									+	+		+			+		+			+						+		+	+	+	+		+	+	
PH 14									+				+								+		+					+					+	+	+
PH 15								+						+	+					+												+	+	+	
PH 16									+	+			+			+		+		+			+		+				+	+	+		+	+	+
PH 17										+		+											+			+						+	+	+	+
PH 18										+							+			+			+								+		+	+	+
PH 19																							+										+	+	+

Гарант освітньо-професійної програми


 Андрій АННИЧ