ПРИЙНЯТО
Рішення вченої ради
Чорноморського національного
університету імені Петра Могили
від 23 січня 2026р.
Протокол № 01

ЗАТВЕРДЖУЮ
23 січня 2026р.
В.о. ректора університету
_____ Леонід КЛИМЕНКО

КОНЦЕПЦІЯ

за спеціальністю F5 «**Кібербезпека та захист інформації**»
галузі знань F «Інформаційні технології»
за освітньо-професійною
програмою «Кібербезпека та захист інформації»
відокремленого структурного підрозділу
«ФАХОВИЙ КОЛЕДЖ ЧОРНОМОРСЬКОГО НАЦІОНАЛЬНОГО
УНІВЕРСИТЕТУ ІМЕНІ ПЕТРА МОГИЛИ»

м. Миколаїв
2026 рік

Концепція
за спеціальністю F5 «Кібербезпека та захист інформації»
галузі знань F «Інформаційні технології»
за освітньо-професійною програмою «Кібербезпека та захист інформації»

Код та найменування спеціальності: F5 «Кібербезпека та захист інформації».
Рівень освіти: фахова передвища освіта.
Освітньо-професійна програма (ОПП): «Кібербезпека та захист інформації».
Обсяг програми: 180 кредитів ЄКТС (термін навчання – 3 роки 10 місяців на основі базової освіти, 2 роки 10 місяців – на основі повної загальної середньої освіти).
Вимоги до вступу: базова або повна загальна середня освіта, професійна (професійно-технічна) освіта.

Концепція освітньо-професійної програми «Кібербезпека та захист інформації» визначає стратегічні засади формування змісту, організації освітнього процесу, очікуваних результатів навчання, методів підготовки здобувачів освіти та орієнтована на сучасні вимоги ринку праці у галузі інженерії програмного забезпечення.

Мета освітньої діяльності: надання теоретичних знань та набуття практичних компетентностей, достатніх для успішного виконання професійних обов'язків у сфері інформаційних технологій та кібербезпеки, підготовка здобувачів освіти до подальшого навчання за обраною спеціалізацією.

Освітній процес у Відокремленому структурному підрозділі «Фаховий коледж Чорноморського національного університету імені Петра Могили» (далі – Коледж) спрямований на формування особистісних компетентностей фахівця, здатного розв'язувати типові спеціалізовані задачі та практичні проблеми кібербезпеки та захисту інформації, що передбачає оволодіння здобувачами знаннями, вміннями та навичками, що пов'язані з розробкою, супроводом та забезпеченням якості програмного забезпечення, баз даних та їх компонентів; створення прикладних програм з використанням процедурного та об'єктно-орієнтованого підходу.

Перелік освітніх компонент, спрямованих на досягнення передбачених освітньою програмою результатів навчання, із зазначенням необхідних засобів для провадження освітньої діяльності

Шифр	Компоненти	Передбачені освітньою програмою результати навчання	Необхідні засоби для провадження освітньої діяльності
1. Нормативні навчальні дисципліни ОПП			
1.1. Цикл загальної підготовки			
ОК1	Іноземна мова (за професійним спрямуванням)*	РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.	Мультимедійний комплект, що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка.
ОК2	Історія та культура України*	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	Мультимедійний комплект, що дозволяє забезпечити проведення

			занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка.
ОК3	Громадянські студії*	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.	Мультимедійний комплект, що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка.
ОК4	Культурологія	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	Мультимедійний комплект, що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка.
ОК5	Основи психології	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка.
ОК6	Фізичне виховання	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	Спортивний інвентар, методичні вказівки до практичних занять.
ОК7	Охорона праці, БЖД та цивільний захист	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	
ОК8	Українська мова (за професійним спрямуванням)	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	Мультимедійний комплект, що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка.

1.2. Цикл професійної підготовки			
ОК9	Інформаційні технології (*Інформатика)	РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.	Мультимедійний комплект, що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.
ОК 10	Основи програмування	РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.	Мультимедійний комплект, що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.
ОК 11	Технології та стандарти інформаційної безпеки (*Технології)	РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних системах відповідно до встановленої політики інформаційної безпеки.	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.

		РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому. РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-телекомунікаційних систем з використання процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту і відновлення інформації. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.	
ОК12	Дискретні структури та дискретна математика*	РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної області кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.
ОК13	Захищені комп'ютерні системи та мережі*	РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських презентаційних

		РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому. РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-телекомунікаційних систем з використання процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту і відновлення інформації. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.	навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.

		РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	
ОК14	Організація баз даних*	РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.
ОК15	Архітектура комп'ютерів	РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. РН8. Застосовувати знання й розуміння математики та фізики в	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення

		професійній діяльності, формалізувати задачі предметної області кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.	занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.
ОК16	Захист IoT-систем	РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.
ОК17	Основи тестування програмного забезпечення та мереж	РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських

		РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.
ОК18	Теорія ймовірностей та математична статистика	РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної області кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.
ОК19	Фізика	РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної області кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення	Мультимедійний комплект, що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.
ОК20	Системи розмежування доступу	РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє

		комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі	забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.

		здійснення процедур кількісної і якісної оцінки ризиків. РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	
ОК21	Основи криптографічного захисту інформації	РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.

		кібербезпеки та захисту інформації у навчанні та професійній діяльності. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.	
ОК22	Комп'ютерні системи*	РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.	Мультимедійний комплект, що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.
ОК23	Безпека веб-застосунків	РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.

		галузі кібербезпеки та захисту інформації. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.	
ОК24	Моніторинг та тестування систем безпеки*	РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.

		реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	
ОК25	Технологія проєктування комп'ютерних систем	РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.

		від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	
ОК26	Захищені вбудовані системи	РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому. РН16. Вирішувати задачі впровадження та супроводу	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп’ютери.

		комплексних систем захисту інформації в інформаційних системах.	
ОК27	Вища математика*	РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран), що дозволяє забезпечити проведення занять з використанням авторських презентаційних навчальних матеріалів та навчальних інтернет-ресурсів; дошка; комп'ютери.
1.3. Цикл практичної підготовки			
ПП01	Навчально-виробнича практика	РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної області кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран).

		кібербезпеки з урахуванням вимог до захисту інформації. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і	

		контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	
ПП02	Передатестаційна практика	РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної області кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. РН12. Застосовувати методи та засоби захисту інформації в	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран).

		інформаційних та інформаційно-телекомунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності	

		систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	
ПП05	Підготовка кваліфікаційної роботи	РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної області кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних системах відповідно до встановленої політики інформаційної безпеки.	Мультимедійний комплект (мультимедійний проєктор, проєкційний екран).

		РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному	

		простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	

Орієнтовний перелік професійних кваліфікацій

Особа, яка здобула ступінь фахової передвищої освіти за освітньо-професійною програмою «Кібербезпека та захист інформації», здатна виконувати професійну роботу (код та назва класифікаційного угрупування професійних назв робіт згідно з Національним класифікатором України ДК 003:2010 (із змінами)): 3119 – технік (сфера захисту інформації), 3439 – фахівець із організації інформаційної безпеки, 3439 – фахівець із організації захисту інформації з обмеженим доступом, 3439 – фахівець з режиму секретності, 3121 – фахівець з інформаційних технологій.

Вимоги до рівня освіти осіб, які можуть розпочати навчання

Наявність свідоцтва про базову (повну) загальну середню освіту (на основі сертифікатів національного мультипредметного тесту або вступних випробувань), а також вступ на старші курси (скорочений термін навчання) на основі диплома кваліфікованого робітника, молодшого спеціаліста, молодшого бакалавра, фахового молодшого бакалавра, бакалавра, спеціаліста, магістра за іншою або спорідненою спеціальністю. Підготовка здійснюється на інституційній формі навчання. Умови вступу визначаються Правилами прийому на навчання до ВСП «Фахового коледжу Чорноморського національного університету імені Петра Могили».

Порядок оцінювання результатів навчання

Контрольні заходи включають поточний та підсумковий контролі успішності, форми якого визначаються навчальними планами та робочими програмами освітніх компонентів.

Критерії оцінювання навчальних досягнень реалізуються в нормах оцінок, які встановлюють співвідношення між вимогами до знань, умінь, комунікації, автономності та відповідальності здобувача фахової передвищої освіти за Національною рамкою кваліфікацій і показником оцінки в балах.

Оцінювання здобувачів вищої освіти здійснюється за рейтинговою шкалою (1-12 балів) та за національною шкалою («відмінно», «добре», «задовільно», «зараховано»).

Атестація здійснюється у формі захисту кваліфікаційної роботи та завершується отриманням документу встановленого зразка про здобуття освітнього ступеня фахового молодшого бакалавра з інженерії програмного забезпечення.

Кваліфікаційна робота передбачає розв’язання типової задачі інженерії програмного забезпечення, що характеризуються певною невизначеністю умов, зі застосуванням теорій та методів інформаційних технологій. Кваліфікаційна робота не повинна містити академічного плагіату, ознак фабрикації та фальсифікації. Кваліфікаційна робота має бути оприлюднена на офіційному сайті Коледжу або його структурного підрозділу, або в репозитарії ЧНУ імені Петра Могили.

Керівник проєктної групи:
викладач вищої категорії, доктор філософії  Олексій ТОГОЄВ