



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека та захист інформації»

першого (бакалаврського) рівня вищої освіти

за спеціальністю F5 Кібербезпека та захист інформації

галузі знань F Інформаційні технології

Кваліфікація: бакалавр з кібербезпеки та захисту інформації



ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ОНМУ

Голова Вченої ради

/Сергій РУДЕНКО/

(протокол № 8 від « 26 » березня 2025 р.)

Освітня програма вводиться в дію з 01 .09. 2025 р.

Ректор _____ /Сергій РУДЕНКО/

(наказ № 105-орг від «27» березня 2025 р.)



Одеса 2025 р.

ПЕРЕДМОВА

I. Освітньо-професійну програму «Кібербезпека та захист інформації» першого (бакалаврського) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації галузі знань F Інформаційні технології розроблено проектною групою на підставі Стандарту вищої освіти України, що затверджений і введений в дію наказом Міністерства освіти і науки України від 29.10.2024 р. №1547, з урахуванням: наказу МОНУ від 13.06.2024 р. № 842, Постанови КМУ «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти» від 30.08.2024 р. № 1021, наказу МОНУ від 19.11.2024 р. № 1625; Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських, затвердженого постановою КМУ від 21.06.2024 р. № 734; пропозицій стейкхолдерів.

II. Склад проектної групи:

1. **Вікторія ЗОРІЛО** – керівник проектної групи (гарант програми), к.т.н, доцент кафедри «Кафедра технічної кібернетики й інформаційних технологій ім. професора Р.В.Меркта» ОНМУ;

2. **Алла КОБОЗЄВА** – д.т.н., професор, професор кафедри «Кафедра технічної кібернетики й інформаційних технологій ім. професора Р.В.Меркта» ОНМУ;

3. **Олена ЛЕБЕДЄВА** – к.т.н, доцент, доцент кафедри «Кафедра технічної кібернетики й інформаційних технологій ім. професора Р.В.Меркта» ОНМУ;

4. **Катерина ТРИФОНОВА** – ст.викл. кафедри «Кафедра технічної кібернетики й інформаційних технологій ім. професора Р.В.Меркта» ОНМУ.

Залучені здобувачі вищої освіти:

Ілля ТОЧИНСЬКИЙ – здобувач другого року навчання за рівнем освіти бакалавр, гр. КБ 21.

Залучені роботодавці:

Денис ПОПОВ – заступник начальника Управління Держспецзв'язку в Одеській області.

III. Рецензії-відгуки на ОП зовнішніх стейкхолдерів:

1. **Володимир ХОРОШКО** – д.т.н., професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету;

2. **Іван БОБОК** – д.т.н., доцент, професор кафедри комп'ютеризованих систем та програмних технологій Національного університету «Одеська політехніка».

Ця освітньо-професійна програма не може бути повністю або частково відтворена, тиражована та розповсюджена без дозволу Одеського національного морського університету.

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ» СПЕЦІАЛЬНОСТІ F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Одеський національний морський університет Навчально-науковий інститут інформаційних технологій та інноваційного підприємництва Кафедра «Кафедра технічної кібернетики та інформаційних технологій ім. професора Р.В.Меркта»
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь – бакалавр Освітня кваліфікація – бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека та захист інформації» підготовки здобувачів вищої освіти першого (бакалаврського) рівня за спеціальністю F5 Кібербезпека та захист інформації галузі знань F Інформаційні технології
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, у тому числі обсяг обов'язкової складової – 177 кредитів ЄКТС. Обсяг, який відводиться на дисципліни за вибором здобувачів, становить 63 кредити ЄКТС (26.25%). Термін навчання: денна форма – 3 роки 10 місяців, заочна – 3 роки 10 місяців.
Наявність акредитації	Акредитується вперше. Національне агентство забезпечення якості вищої освіти. Україна. Строк подання програми на акредитацію – 2027 р.
Цикл / рівень	Перший (бакалаврський) рівень, НРК України – 6 рівень, EQF-LLL – 6 рівень, FQ-EHEA – перший цикл.
Передумови	Наявність документу про загальну середню освіту або диплому ОКР «Молодший бакалавр». Решта вимог визначаються Правилами прийому до Одеського національного морського університету.
Мова(и) викладання	Українська
Термін дії освітньої програми	2025-2029 (або до наступного необхідного оновлення)
Інтернет-адреса постійного розміщення опису освітньої програми	https://onmu.org.ua/ua/vibir-sp-bachelor.html
2 – Мета освітньо-професійної програми	
Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та кібербезпеки за умови набуття загальних та оволодіння системою фахових (спеціальних) компетентностей, що є основою конкурентоспроможності випускників на ринку праці.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	<i>Галузь знань</i> – F Інформаційні технології. <i>Спеціальність</i> – F5 Кібербезпека та захист інформації. <i>Об'єкти професійної діяльності</i> – 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. Цілі навчання – підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв’язувати складні задачі у галузі кібербезпеки та захисту інформації. Теоретичний зміст предметної області – принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Методи, методики та технології – методи, методики та технології розв’язання теоретичних і практичних задач кібербезпеки та захисту інформації. Інструменти та обладнання – засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків)
Орієнтація освітньої програми	Освітньо-професійна програма. Має прикладну орієнтацію та спрямована на набуття здобувачами вищої освіти профільно-орієнтованих компетентностей з кібербезпеки та захисту інформації, зокрема для забезпечення неперервності функціонування критичної інфраструктури держави.
Основний фокус освітньої програми та спеціалізації	Вища освіта та професійна підготовка фахівців з кібербезпеки та захисту інформації, зокрема в сфері критичної інфраструктури держави, набуття компетентностей, пов’язаних з захистом складових кіберпростору, спеціалізованими та практичними задачами у галузі забезпечення інформаційної та кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов. <i>Ключові слова:</i> кібербезпека, захист інформації, інформаційна безпека держави.
Особливості програми	Характерною особливістю програми є надання можливості поглибленого вивчення дисциплін, присвячених розробці та використанню спеціалізованого програмного забезпечення, зокрема в сфері водного транспорту.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Після здобуття кваліфікації бакалавра з кібербезпеки та захисту інформації випускники можуть працевлаштуватися в державному та приватному секторах у різних сферах діяльності, зокрема: на підприємствах (зокрема морської галузі), в установах, організаціях. Основні посади згідно з Національним класифікатором України «Класифікатор професій ДК 003:2010» від 28.07.2010 р. (із змінами 2019 р.), які можуть обіймати випускники: КП 3121 Фахівець з інформаційних технологій; КП 3439 Інспектор з організації захисту секретної інформації; КП 3439 Фахівець з режиму секретності; КП 3439 Фахівець із організації захисту інформації з обмеженим доступом; КП 3439 Фахівець із організації інформаційної безпеки.

Подальше навчання	Продовження навчання на другому (магістерському) рівні вищої освіти (для отримання освітнього ступеня «магістр»).
5 – Викладання та оцінювання	
Викладання та навчання	<i>Основні підходи до навчання:</i> студенто-центроване навчання, самонавчання. <i>Методи навчання:</i> дослідницький, проблемний, ситуаційний, дискусійний. <i>Освітні технології:</i> навчання через дослідження.
Оцінювання	Оцінювання успішності навчання здійснюється за 100 бальною системою: за національною шкалою («відмінно», «добре», «задовільно», «незадовільно») та Європейською кредитною трансфертно-накопичувальною системою ECTS («А», «В», «С», «D», «Е», «FX», «F»). <i>Види контролю:</i> поточний, підсумковий. Поточний контроль – опитування, тестовий контроль, презентація індивідуальних завдань, курсові роботи, звіти з практики. Підсумковий контроль – екзамени та заліки з урахуванням накопичених балів поточного контролю. Атестація – єдиний державний кваліфікаційний іспит; підготовка та захист кваліфікаційної роботи.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (ЗК)	Компетентності, визначені стандартом вищої освіти спеціальності: ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК4. Здатність спілкуватися іноземною мовою. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні. ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК8. 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. Компетентності, визначені ОНМУ: ЗК9. Здатність здобувати вищу освіту з дотриманням вимог законодавства, стандартів освіти та внутрішніх нормативних документів ОНМУ та здатність використовувати інформаційні технології і спеціалізоване програмне забезпечення, інтегроване в освітнє середовище ОНМУ.

	ЗК10. Здатність реалізовувати свої права і обов'язки як студента ОНМУ під час навчання, проживання в гуртожитках та під час позанавчальної діяльності.
Спеціальні (фахові, предметні) компетентності (СК)	Компетентності, визначені стандартом вищої освіти спеціальності: СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності. СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів й походження. СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.) СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки. Компетентності, визначені ОНМУ: СК11. Здатність аналізувати, виявляти та усувати загрози, уразливості, наслідки кібератак в сфері критичної інфраструктури, зокрема водного транспорту.
7 – Програмні результати навчання	
Програмні результати навчання (РН)	Програмні результати навчання, визначені стандартом вищої освіти спеціальності: РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач й 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.

РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН7. Застосовувати та 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.

РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі 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 й засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН13. Впроваджувати, налаштовувати, супроводжувати й підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних і інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.

РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки й забезпечувати функціонування спеціального програмного забезпечення щодо захисту і відновлення інформації.

РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах;

РН17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал й 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 й 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 і використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах. Програмні результати навчання, визначені ОНМУ: РН22. Вирішувати задачі аналізу, виявлення та усунення загроз, уразливостей, наслідків кібератак в сфері критичної інфраструктури, зокрема водного транспорту. РН23. Використовувати інформаційні технології і спеціалізоване програмне забезпечення, інтегроване в освітнє середовище ОНМУ, дотримуватися вимог законодавства, стандартів освіти та внутрішніх нормативних документів ОНМУ під час здобуття вищої освіти. РН24. Усвідомлювати і реалізовувати свої права і обов'язки як студента ОНМУ під час навчання, проживання в гуртожитках та під час позанавчальної діяльності.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Усі науково-педагогічні працівники, що задіяні в реалізації освітньої програми, відповідають кадровим вимогам ліцензійних умов провадження освітньої діяльності закладів освіти. Гарант ОПП: Зоріло Вікторія Вікторівна, кандидат технічних наук, доцент кафедри «Технічної кібернетики й інформаційних технологій імені професора Р.В.Меркта». В освітньому процесі беруть участь доктори та кандидати наук, професори та доценти, старші викладачі та асистенти (спеціальність «Системи захисту інформації»). У навчального процесу задіюються професіонали-практики з інформаційної та кібербезпеки.
Матеріально-технічне забезпечення	Усі приміщення відповідають будівельним та санітарним нормам; 100% здобувачів (відповідно до потреби) забезпечені гуртожитками, соціальною інфраструктурою, що включає спортивний комплекс, пункти харчування, медпункт тощо; наявність профільних аудиторій, лабораторій, які обладнані комп'ютерами, серверами та іншим обладнанням, прикладним програмним забезпеченням, що використовується для досліджень в галузі кібербезпеки і є достатніми для виконання навчальних планів; наявна соціальна інфраструктура, що включає спортивний комплекс, пункти харчування, медпункт тощо.
Інформаційне та навчально-методичне забезпечення	Належна забезпеченість бібліотеки підручниками та навчальними посібниками, вітчизняними і закордонними фаховими періодичними виданнями, доступ до джерел Internet, авторські розробки професорсько-викладацького складу. Офіційний веб-сайт https://onmu.org.ua/ua/biblioteka-2.html містить

	загальну інформацію про навчальне, наукове, методичне середовище, структурні підрозділи, правила прийому, контакти тощо. В ОНМУ є локальна комп'ютерна мережа з необмежним доступом до мережі Інтернет. Користування Інтернет-мережею безлімітне. Передбачено використання авторських розробок професорсько-викладацького складу. Матеріали навчально-методичного забезпечення освітньої програми викладені у внутрішній електронній мережі. На платформі MOODLE викладено навчально-методичне забезпечення по кожній компоненті навчального плану: конспект лекцій, методичні рекомендації до виконання практичних (лабораторних) робіт, методичні рекомендації до виконання самостійної роботи студентів та інше, з яким студент може працювати, маючи власний код доступу.
9 – Академічна мобільність	
Національна кредитна мобільність	Національна кредитна мобільність здобувачів вищої освіти, наукових і науково-педагогічних працівників, у т.ч. навчання, стажування, проведення наукових досліджень, викладання та підвищення кваліфікації організовується відповідно до Положення про реалізацію права на академічну мобільність в Одеському національному морському університеті, Положення про організацію освітнього процесу в Одеському національному морському університеті та партнерських угод про співпрацю між Одеським національним морським університетом та закладами вищої освіти в Україні. В ОНМУ працює Центр міжвузівської освіти, місія якого – створення умов для організації та розширення співпраці між здобувачами вищої освіти та викладачами ОНМУ з іншими навчальними закладами, у тому числі з іноземними партнерами.
Міжнародна кредитна мобільність	Робота Центру міжвузівської освіти ОНМУ з закордонними ЗВО здійснюється відповідно до міжуніверситетських угод. Міжнародна кредитна мобільність в ОНМУ регулюється: Положенням про реалізацію права на академічну мобільність в Одеському національному морському університеті; Положенням про організацію освітнього процесу в Одеському національному морському університеті; Положенням про Центр міжвузівської освіти в Одеському національному морському університеті. В ОНМУ створені широкі можливості для здійснення академічної мобільності до університетів ЄС у рамках програми Erasmus+ K1, здійснення самоініційованої мобільності (Центр Східноєвропейських студій. Асоціація європейських університетів - EUA).
Навчання іноземних здобувачів вищої освіти	Освітня програма передбачає можливості навчання іноземних громадян за умови акредитації ОПП та відповідно до Правил прийому до ОНМУ.

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1. Перелік компонент освітньої програми «Кібербезпека та захист інформації»

Дана освітньо-професійна програма передбачає виділення дисциплін двох видів: обов'язкових дисциплін (177 кредитів) (цикл загальної підготовки та цикл дисциплін професійної та практичної підготовки), а також дисциплін за вільним вибором здобувача (63 кредити), які вони можуть самостійно обирати (3-8 семестри).

У таблиці 1 надано розподіл змісту освітньо-професійної програми з урахуванням навчального часу та кількості кредитів ЄКТС за обов'язковими дисциплінами та дисциплінами вільного вибору здобувачів.

У даній освітній програмі одному навчальному року відповідає 60 кредитів ЄКТС. Одному кредиту ЄКТС відповідають 30 годин загального навчального навантаження здобувача.

Таблиця 2.1 – Структура освітньо-професійної програми

Код компо- ненти	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Семестр
1. ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ				
1.1. Цикл дисциплін загальної підготовки				
ОК 1	Фізика	5	екзамен	1
ОК 2	Вища математика	12	екзамен / екзамен	1,2
ОК 3	Українська мова (за професійним спрямуванням)	3	екзамен	2
ОК 4	Англійська мова (за професійним спрямуванням)	3	залік	3
ОК 5	Філософія	3	екзамен	4
ОК 6	Теорія ймовірності, ймовірнісні процеси та математична статистика	4	екзамен	3
ОК 7	Історія і культура України	4	залік	2
ОК 8	Людина. Суспільство. Держава.	3	залік	6
ОК 9	Вступ до фаху	3	залік	1
Загальний обсяг компонент загальної підготовки		40		
1.2. Цикл дисциплін професійної та практичної підготовки				
ОК 10	Нормативно-правове та організаційне забезпечення захисту інформації	4	екзамен	1
ОК 11	Програмування	9	залік/екзамен	1,2
ОК 12	Спеціальні розділи математики в кібербезпеці	9	залік/екзамен	1,2
ОК 13	Інформаційна безпека держави	6	екзамен	1,2
ОК 14	Операційні системи та системне програмування	5	залік	2
ОК 15	Схемотехніка та архітектура комп'ютерів	4	залік	3
ОК 16	Об'єктно-орієнтоване програмування	5	екзамен	3
ОК 17	Спеціальні розділи програмування	6	екзамен	3

ОК 18	Бази даних та їх захист	4	екзамен	4
ОК 19	Інформаційно-телекомунікаційні системи та їх захист	8	екзамен/ залік	4,5
ОК 20	Цифрова криміналістика	5	екзамен	6
ОК 21	Комп'ютерна вірусологія та антивірусне програмне забезпечення	3	екзамен	5
ОК 22	Програмно-технічні засоби захисту інформації	6	залік/ екзамен	4,5
ОК 23	Комплексні системи захисту інформації	5	екзамен	5
ОК 24	Управління ризиками	4	екзамен	5
ОК 25	Основи криптографії	6	екзамен	6
ОК 26	Управління доступом	4	екзамен	7
ОК 27	Методи оцінки захищеності інформаційних систем	4	екзамен	7
ОК 28	Основи стеганографії	4	залік	7
ОК 29	Управління та обробка інцидентів кібербезпеки	4	екзамен	8
ОК 30	Критична інфраструктура України та її інформаційна безпека	3	залік	7
ОК 31	Мережева та інформаційна безпека в морському секторі	3	залік	7
ОК 32	Управління кібербезпекою	4	екзамен	7
ОК 33	Виробнича практика	4	залік	6
ОК 34	Переддипломна практика	7	залік	8
ОК 35	Єдиний державний кваліфікаційний іспит	2	екзамен	8
ОК 36	Кваліфікаційна робота	9	екзамен	8
Загальний обсяг компонент професійної підготовки		137		
Загальний обсяг обов'язкових компонент		177 кредитів / 5310 годин		
2. ЦИКЛ ДИСЦИПЛІН ВИБОРУ СТУДЕНТА				
ВИБІРКОВІ ДИСЦИПЛІНИ ПРОФЕСІЙНОЇ І ПРАКТИЧНОЇ ПІДГОТОВКИ				
2.1. Дисципліни циклу БЗВП				
Відповідно до Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських, затвердженого постановою Кабінету Міністрів України № 734 від 21 червня 2024 року три кредити ЄКТС із загального обсягу вільного вибору спрямовано на реалізацію освітнього компонента «Теоретична підготовка базової загальновійськової підготовки».				
Всього		3 кредити		
2.2. Дисципліни циклу за ОП				
Дисципліни вільного вибору професійної підготовки обираються здобувачами з каталогу вибіркового дисциплін за освітньо-професійною програмою «Кібербезпека та захист інформації» на першому (бакалаврському) рівні. Кожен вибіркового компонент має 4 кредити. Каталог вибіркового дисциплін розміщено у відкритому доступі.				
Всього		36 кредитів		
2.3. Дисципліни загальноуніверситетського циклу та інших освітніх програм				
Дисципліни загальноуніверситетського циклу та інших освітніх програм ОНМУ обираються здобувачами з каталогу вибіркового дисциплін. Кожен вибіркового компонент має 4 кредити. Каталог вибіркового дисциплін ОНМУ розміщено у відкритому доступі на офіційному сайті університету.				
Всього		24 кредити		
Загальний обсяг вибіркового компонент		63 кредити / 1890 годин		
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240 кредитів / 7200 годин		

Згідно із Законом України «Про вищу освіту» здобувачі вищої освіти мають право на «вибір навчальних дисциплін у межах, передбачених відповідною освітньою програмою та робочим навчальним планом, в обсязі, що становить не менш як 25% загальної кількості кредитів ЄКТС, передбачених для даного рівня вищої освіти. При цьому здобувачі певного рівня вищої освіти мають право вибирати навчальні дисципліни, що пропонуються для інших рівнів вищої освіти, за погодженням з керівником відповідного факультету чи підрозділу».

Починаючи з 3-го семестру та протягом 4, 5, 6, 7 та 8-ого семестрів здобувачі вищої освіти можуть самостійно обирати дисципліни із Каталогу ОП, який розміщений у вільному доступі, а також Каталогу загальноуніверситетського, який розміщений в системі Moodle. Після обрання здобувачем освітньої компоненти, вона становиться обов'язковою для вивчення.

2.2. Розподіл змісту ОП за групами компонент

№ з/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів / %)		
		Обов'язкові компоненти ОП	Вибіркові компоненти ОП	Всього за весь термін навчання
1	Цикл дисциплін загальної підготовки	40 / 16,67	24 / 10	64 / 26,67
2	Цикл дисциплін професійної підготовки	137 / 57,08	39 / 16,25	176 / 73,33
3	Всього за весь термін навчання	177 / 73,75	63 / 26,25	240 / 100

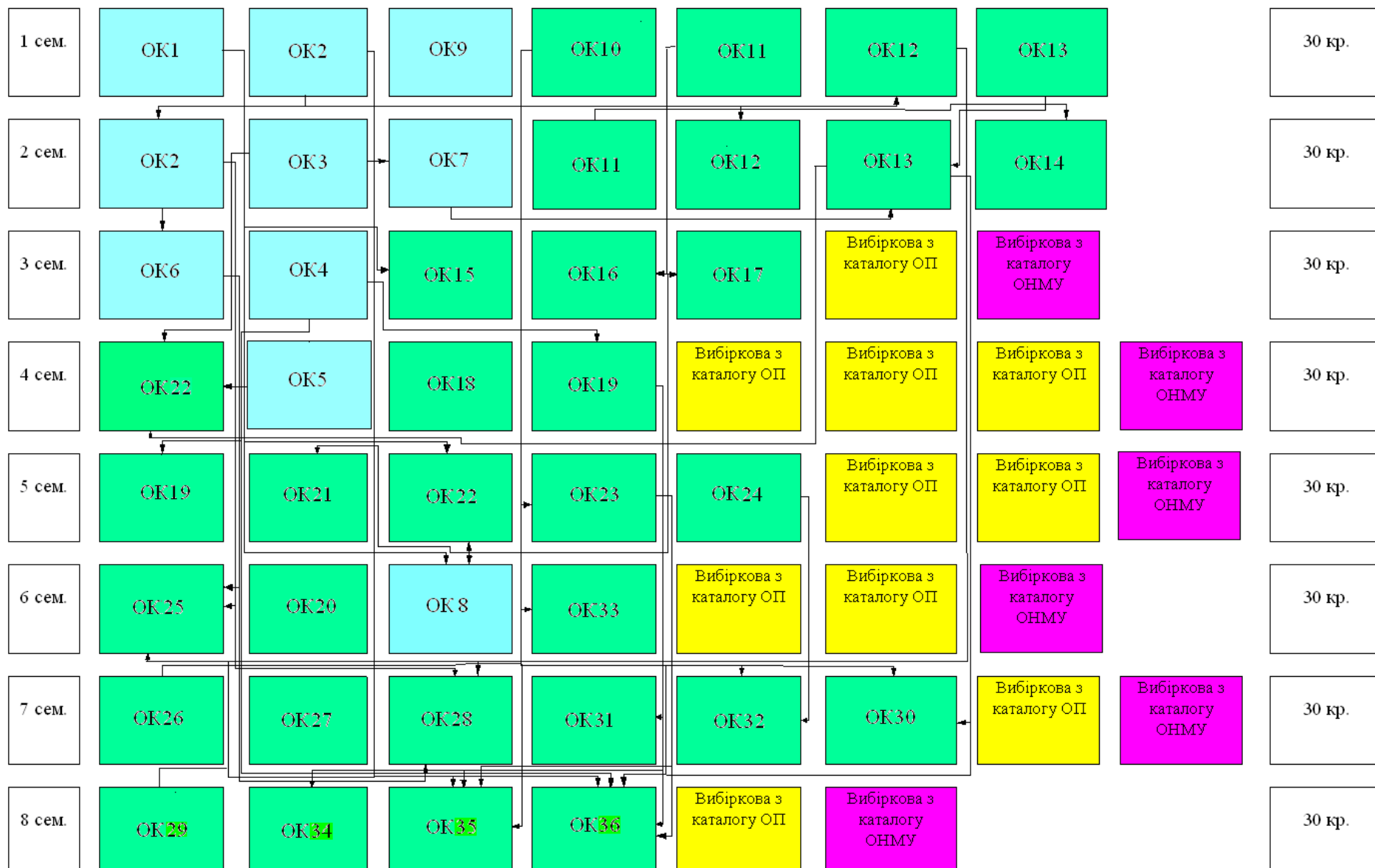
2.3. Структурно-логічна схема освітньо-професійної програми

Розподіл дисциплін за циклами, послідовність їх вивчення, розподіл кредитів, конкретні форми проведення навчальних занять (лекції, практичні, семінарські, індивідуальні заняття, консультації, практики) та їх обсяг, графік навчального процесу, форми підсумкового контролю визначені навчальним планом.

Короткий опис логічної послідовності вивчення освітніх компонентів освітньо-професійної програми надано в таблиці 2 та на рис. 1.

Таблиця 2.2. Логічна послідовність вивчення ОК ОПП за семестрами

Семестр	Види навчальної діяльності
I	ОК 1 (5 кредити), ОК 2 (6), ОК 9 (3), ОК 10 (4), ОК 11 (4), ОК 12 (5), ОК 13 (3)
II	ОК 2 (6 кредитів), ОК 3 (3), ОК 7 (4), ОК 11 (5), ОК 12 (4), ОК 13 (3), ОК 14 (5)
III	ОК 4 (3 кредити), ОК 6 (4), ОК 15 (4), ОК 16 (5), ОК 17 (6), <u>ВВ ОП (4), ВВ ОНМУ (4)</u>
IV	ОК 5 (3 кредити), ОК 18 (4), ОК 19 (5), ОК 22 (3), <u>ВП ОП (11), ВВ ОНМУ (4)</u>
V	ОК 19 (3 кредити), ОК 21 (3), ОК 22 (3), ОК 23 (5), ОК 24 (4), <u>ВП ОП (8), ВВ ОНМУ (4)</u>
VI	ОК 8 (3), ОК 20 (5 кредити), ОК 25 (6), ОК 33 (4), <u>ВП ОП (8), ВВ ОНМУ (4)</u>
VII	ОК 26 (4 кредити), ОК 27 (4), ОК 28 (4), ОК 30 (3), ОК 31 (3), ОК 32 (4), <u>ВВ ОП (4), ВВ ОНМУ (4)</u>
VIII	ОК 29 (4 кредити), ОК 34 (7), ОК 35 (2), ОК 36 (9), <u>ВВ ОП (4), ВВ ОНМУ (4)</u>



Умовні позначення: OK1 - Обов'язкові компоненти ОП (цикл дисциплін загальної підготовки); OK10 - Обов'язкові компоненти ОП (цикл дисциплін професійної та практичної підготовки); Вибіркова з каталогу ОП - Вибіркові компоненти ОП (з каталогу ОП) Вибіркова з каталогу ОНМУ - Вибіркові компоненти ОП (з каталогу ОНМУ)

Рис.1 Структурно-логічна схема ОПП «Кібербезпека та захист інформації»

3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників ОП «Кібербезпека та захист інформації» спеціальності F5 Кібербезпека та захист інформації здійснюється у формі: єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи й завершується видачею документа встановленого зразка про присудження здобувачеві освітнього ступеня бакалавра з присвоєнням кваліфікації: бакалавр з кібербезпеки та захисту інформації.

Вимоги до єдиного державного кваліфікаційного іспиту: Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом вищої освіти.

Кваліфікаційна робота на здобуття освітнього ступеня бакалавр зі спеціальності F5 Кібербезпека та захист інформації ОП «Кібербезпека та захист інформації» є самостійним розгорнутим дослідженням. Кваліфікаційна робота передбачає розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації.

У кваліфікаційній роботі не повинно бути академічного плагіату, фальсифікації та фабрикації.

Атестація здобувачів у формі захисту кваліфікаційної роботи здійснюється відкрито і публічно. До захисту допускаються кваліфікаційні роботи, виконані здобувачем самостійно із дотриманням принципів академічної доброчесності.

Кваліфікаційна робота розміщується в репозитарії ОНМУ.

4. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ПРОГРАМНИМ КОМПЕТЕНТНОСТЯМ

[illegible]

5. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ (ПРН) ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

[illegible]

6. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Програмні компетент- ності	Шифри освітніх компонент ОПП																																					
	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	ОК 36		
ЗК1	+	+			+	+					+	+				+	+		+		+						+	+	+					+	+	+	+	
ЗК2									+						+												+	+			+				+	+	+	+
ЗК3			+																																+	+	+	+
ЗК4				+																																		+
ЗК5	+	+				+					+	+				+	+																		+	+	+	+
ЗК6							+	+		+			+																						+	+	+	+
ЗК7							+	+		+			+																						+	+	+	+
ЗК8							+	+																											+	+	+	+
ЗК9									+																											+	+	+
ЗК10									+																													
СК1										+			+							+											+				+	+	+	+
СК2											+	+		+		+	+		+	+	+				+				+					+	+	+	+	
СК3																			+					+												+	+	+
СК4														+	+			+	+		+	+	+									+		+	+	+	+	
СК5																			+	+	+									+		+	+	+	+	+	+	
СК6																							+													+	+	+
СК7																								+						+			+			+	+	+
СК8																										+									+	+	+	+
СК9																						+													+	+	+	+
СК10																			+		+		+				+	+							+	+	+	+
СК11																															+	+				+	+	+