



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека та захист інформації»

другого (магістерського) рівня вищої освіти

за спеціальністю F5 Кібербезпека та захист інформації

галузі знань F Інформаційні технології

Кваліфікація: магістр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ОНМУ

Голова Вченої ради

_____/Сергій РУДЕНКО/

(протокол № 5 від «18» грудня 2024 р.)

Освітня програма вводиться в дію з 01.09.2025 р.

Ректор _____/Сергій РУДЕНКО/

(наказ № 494-орг від «23» грудня 2024 р.)



Одеса 2024 р.

ПЕРЕДМОВА

I. Освітньо-професійну програму «Кібербезпека та захист інформації» другого (магістерського) 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 18.03.2021 р. №332, 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:

Члени проектної групи:

Керівник проектної групи:

Олена ЛЕБЕДЄВА, к.т.н., доцент, доцент кафедри технічної кібернетики й інформаційних технологій ім.професора Р.В.Меркта Одеського національного морського університету (гарант програми).

Члени проектної групи:

Алла КОБОЗЄВА, д.т.н., професор, професор кафедри кібернетики й інформаційних технологій ім.професора Р.В.Меркта Одеського національного морського університету

Вікторія ЗОРИЛО, к.т.н., доцент кафедри кібернетики й інформаційних технологій ім.професора Р.В.Меркта Одеського національного морського університету

Микола МАЛАКСІАНО, д.т.н., професор, завідувач кафедри кібернетики й інформаційних технологій ім.професора Р.В.Меркта Одеського національного морського університету.

Залучені здобувачі вищої освіти:

Ілля ТОЧИНСЬКИЙ – гр.КБ бак 21, другого року навчання

Андрій РОМАНОВ – аспірант четвертого року навчання

Залучені роботодавці:

Денис ПОПОВ - заступник начальника Управління Держспецзв'язку в Одеській області

III. Рецензії-відгуки на ОП зовнішніх стейкхолдерів:

Хорошко Володимир Олексійович – доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету;

Бобок Іван Ігорович – доктор технічних наук, 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 «Технічної кібернетики та інформаційних технологій ім. професора Р.В.Меркта»	
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь - магістр, Освітня кваліфікація - магістр з кібербезпеки та захисту інформації.	
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації галузі знань F Інформаційні технології.	
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, у тому числі обсяг обов'язкової складової - 62 кредити ЄКТС. Обсяг, який відводиться на дисципліни за вибором здобувачів, становить 28 кредитів ЄКТС (31,1%). Термін навчання: денна форма - 1 рік 4 місяці.	
Наявність акредитації	Акредитується вперше. Національне агентство забезпечення якості вищої освіти. Україна. Строк подання програми на акредитацію – 2026 р.	
Цикл / рівень	Другий (магістерський) рівень, НРК України - 7 рівень, EQF-LLL – 6 рівень, FQ-EHEA - другий цикл.	
Передумови	Наявність диплому ОКР «бакалавр». Решта вимог визначається Правилами прийому до Одеського національного морського університету.	
Мова(и) викладання	Українська	
Термін дії освітньої програми	2025-2026 рр. (або до наступного необхідного оновлення)	
Інтернет-адреса постійного розміщення опису освітньої програми	https://onmu.org.ua/ua/vibir-specialty-master.html	
2. Мета освітньої програми		
Забезпечення розвитку професійних, творчих здібностей, приумноження інтелектуального потенціалу здобувачів щодо поглиблення теоретичних і практичних знань, умінь та навичок, підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері кібербезпеки та захисту інформації, що є основою конкурентоспроможності випускників на ринку праці.		
3. Характеристика освітньої програми		
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань - F Інформаційні технології. Спеціальність - F5 Кібербезпека та захист інформації. Об'єкти вивчення - сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; інфраструктура об'єктів інформаційної діяльності	

	та критичних інфраструктур; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; системи управління інформаційною безпекою та/або кібербезпекою; технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. Теоретичний зміст предметної області - Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорія ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. Методи, методики та технології - Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. Інструменти та обладнання - Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньої програми	Освітньо-професійна програма. Програма орієнтована на сучасні тенденції розвитку в сфері кібербезпеки та захисту інформації, пропонує комплексний підхід до здійснення дослідницької діяльності та реалізує це через навчання та практичну підготовку. Освітні компоненти, включені в програму, орієнтовані на актуальні напрями інформаційної безпеки, в межах яких можлива подальша професійна та наукова кар'єра здобувача.
Основний фокус освітньої програми та спеціалізації	Програма спрямована на отримання компетентностей, пов'язаних з захистом складових кіберпростору, шляхом використання сучасних інформаційних технологій, унікальних, в тому числі авторських, математичних підходів в сфері кібербезпеки та захисту інформації, зокрема критичної інфраструктури. <i>Ключові слова:</i> кібербезпека, захист інформації, критична інфраструктура.
Особливості програми	Характерною особливістю даної програми є її орієнтованість на сучасні інформаційні технології та унікальні в галузі кібербезпеки та захисту інформації математичні підходи, їх застосування для розв'язку задач кібербезпеки, зокрема в сфері водного транспорту.
4. Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Після здобуття кваліфікації магістра з кібербезпеки та захисту інформації випускники можуть працевлаштовуватися в державному та приватному секторах у різних сферах діяльності, зокрема на підприємствах (в тому числі, морської галузі), в установах, організаціях. Основні посади згідно з Національним класифікатором України «Класифікатор професій ДК003:2010» від 28.07.2010 р. (із змінами 2019 р.), які можуть обіймати випускники: КП 1210.1 - Керівник підприємства (установи, організації) (сфера захисту інформації) КП 1226.2 - Керівник структурного підрозділу (сфера захисту інформації) КП 1226.2 - Начальник відділення (сфера захисту інформації) КП 1495 - Менеджер (управитель) систем з інформаційної безпеки

	КП 2149.2 - Професіонал із організації захисту інформації з обмеженим доступом КП 2149.2 - Професіонал із організації інформаційної безпеки КП 2149.2 - Розробник систем (крім комп'ютерів) КП 2149.2 - Фахівець (сфера захисту інформації) КП 2149.2 - Інженер з керування й обслуговування систем КП 2132.2 - Програміст прикладний 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 третьому (освітньо-науковому) рівні вищої освіти
5. Викладання та оцінювання	
Викладання та навчання	<i>Основні підходи до навчання:</i> студентоцентроване навчання, самонавчання. <i>Методи навчання:</i> проблемно-орієнтований, дослідницький, ситуаційний, дискусійний. <i>Освітні технології:</i> навчання через дослідження. Навчання з використанням дистанційних технологій. В освітньому процесі ОНМУ використовується система управління дистанційними курсами СУДК «MOODLE».
Оцінювання	Оцінювання успішності навчання здійснюється за 100-бальною системою: за національною шкалою («відмінно», «добре», «задовільно», «незадовільно») та Європейською кредитною трансферно-накопичувальною системою ECTS («А», «В», «С», «D», «Е», «FX», «F»). <i>Види контролю:</i> поточний, підсумковий, атестація. Поточний контроль – опитування, тестовий контроль, презентація індивідуальних завдань, захист курсових робіт, звіти з практики. Підсумковий контроль – екзамени та заліки з урахуванням накопичених балів поточного контролю. Атестація – підготовка та захист кваліфікаційної роботи. Система оцінювання будується на умовах академічної доброчесності та прозорості.
6. Програмні компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (КЗ)	КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Спеціальні (фахові, предметні) компетентності (КФ)	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління

	інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. КФ11. Здатність розробляти, впроваджувати, контролювати систему управління кібербезпекою на водному транспорті.
7. Програмні результати навчання	
Програмні результати навчання (РН)	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес/операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби

інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів у сфері інформаційної та/або кібербезпеки в цілому.

РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.

РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН21. Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

РН24. Аналізувати, розробляти і супроводжувати систему управління кібербезпекою на водному транспорті.

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: Лебедева Олена Юріївна, кандидат технічних наук, доцент, 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 процесі задіюються професіонали-практики з інформаційної та кібербезпеки. Усі науково-педагогічні працівники систематично проходять підвищення кваліфікації у провідних університетах України, в межах міжнародних проектів в сфері кібербезпеки, на профільних підприємствах. Практикується систематичне підвищення кваліфікації на курсах з поглиблення професіоналізму.
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, сучасним мережевим та іншим обладнанням, прикладним програмним забезпеченням, що використовується для досліджень в галузі кібербезпеки і є достатнім для виконання навчальних планів.
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.odessa.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

Дана освітньо-професійна програма передбачає виділення дисциплін двох видів: обов'язкових дисциплін (цикл загальної підготовки та цикл дисциплін професійної та практичної підготовки – 62 кредити), а також дисциплін за вільним вибором здобувача (28 кредитів).

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

У таблиці 2.1 надано розподіл змісту освітньо-професійної програми з урахуванням навчального часу та кількості кредитів ЄКТС за обов'язковими дисциплінами та дисциплінами вільного вибору здобувачів.

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

Таблиця 2.1 – Структура освітньо-професійної програми

Код компоненти	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Семестр
1. ОBOB'ЯЗKОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ				
1.1. Цикл дисциплін загальної підготовки				
OK1	Професійна англійська мова	3	залік	1
OK2	Методологія наукових досліджень в ІТ-галузі	3	екзамен	1
Загальний обсяг компонент загальної підготовки		6		
1.2. Цикл дисциплін професійної та практичної підготовки				
OK3	Сучасні КСЗІ та їх особливості	4	екзамен, КР	1
OK4	Бізнес-процеси в кібербезпеці	5	екзамен	1
OK5	Проблеми кібербезпеки та сучасні підходи до їх вирішення	5	екзамен	1
OK6	Управління кібербезпекою та захист інформаційних мереж на судні	6	екзамен	2
OK7	Захист соціо-технічних систем	3	залік	1
OK8	Програмна обробка та аналіз даних	4	залік	1
OK9	Інформаційно-аналітичне забезпечення інформаційної безпеки	3	залік	1
OK10	Сучасні методи захисту комп'ютерних	4	екзамен	2

	мереж			
OK11	Переддипломна практика	15	залік	3
OK12	Кваліфікаційна (магістерська) робота	7	екзамен	3
Загальний обсяг компонент професійної підготовки		56		
Загальний обсяг обов'язкових компонент		1860 годин / 62 кредити		
2. ЦИКЛ ДИСЦИПЛІН ВИБОРУ СТУДЕНТА				
ВИБІРКОВІ ДИСЦИПЛІНИ ПРОФЕСІЙНОЇ І ПРАКТИЧНОЇ ПІДГОТОВКИ				
2.1. Дисципліни циклу за ОП				
Дисципліни вільного вибору професійної підготовки обираються здобувачами з каталогу вибіркових дисциплін за освітньо-професійною програмою «Кібербезпека та захист інформації» на другому (магістерському) рівні. Кожен вибірковий компонент має 4 кредити. Каталог вибіркових дисциплін розміщено у відкритому доступі на офіційному сайті університету.				
Всього		20 кредитів		
2.2. Дисципліни загальноуніверситетського циклу та інших освітніх програм				
Дисципліни загальноуніверситетського циклу та інших освітніх програм ОНМУ обираються здобувачами з каталогу вибіркових дисциплін. Кожен вибірковий компонент має 4 кредити. Каталог вибіркових дисциплін ОНМУ розміщено у відкритому доступі на офіційному сайті університету.				
Всього		8 кредитів		
Загальний обсяг вибіркових компонент		840 годин / 28 кредитів		
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		2700 годин / 90 кредитів		

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». Здобувачі вищої освіти можуть самостійно обирати дисципліни із Каталогу, який розміщений у вільному доступі на офіційному сайті ЗВО. Після обрання здобувачем дисципліни вона стає обов'язковою для вивчення.

2.2. Розподіл змісту ОП за групами компонент

№ п/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	6 / 6,67	8 / 8,89	14 / 15,56
2	Цикл дисциплін професійної підготовки	56 / 62,22	20 / 22,22	76 / 84,44
3	Всього за весь термін навчання	62 / 68,89	28 / 31,11	90 / 100

2.3. Структурно-логічна схема освітньо-професійної програми «Кібербезпека та захист інформації»

Розподіл дисциплін за циклами, послідовність їх вивчення, розподіл кредитів, конкретні форми проведення навчальних занять 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 2.2 та на рис. 2.1.

Таблиця 2.2. Логічна послідовність вивчення освітніх компонентів освітньо-професійної програми по семестрах

Семестр	Види навчальної діяльності
I	ОК 1 (3 кредити), ОК 2 (3), ОК 3 (4), ОК 4 (5), ОК 5 (5), ОК 7 (3), ОК 8 (4), ОК 9 (3)
II	ОК 6 (6), ОК 10 (4), <u>ВД ОП (20)</u>
III	ОК 11 (15), ОК 12 (7), <u>ВД ОНМУ (8)</u>



Умовні позначення:

■ - обов'язкові компоненти ОП (цикл дисциплін загальної підготовки);

■ - обов'язкові компоненти ОП (цикл дисциплін професійної та практичної підготовки);

■ - вибіркові компоненти ОП (з каталогу вибіркових дисциплін професійної та практичної підготовки)

■ - вибіркові компоненти ОП (з каталогу вибіркових дисциплін загальноуніверситетського циклу та інших освітніх програм)

Рис.2.1. Структурно-логічна схема ОПП «Кібербезпека та захист інформації»

3 ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

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

Кваліфікаційна робота на здобуття освітнього ступеня магістр зі спеціальності F5 Кібербезпека та захист інформації ОП «Кібербезпека та захист інформації» є самостійним розгорнутим дослідженням. Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій.

Обсяг роботи – до 70 сторінок (не враховуючи додатки).

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 репозиторії ОНМУ.

4 МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ПРОГРАМНИМ КОМПЕТЕНТНОСТЯМ

[illegible]

5 МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

Програмні результати навчання	Шифри освітніх компонент ОПП											
	OK1	OK2	OK3	OK4	OK5	OK6	OK7	OK8	OK9	OK10	OK11	OK12
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				+			+				+	+
PH 20						+					+	+
PH 21					+		+			+	+	+
PH 22					+						+	+
PH 23			+			+					+	+
PH 24						+					+	+

6 МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Програмні компетент ності	Шифри освітніх компонент ОПП											
	OK1	OK2	OK3	OK4	OK5	OK6	OK7	OK8	OK9	OK10	OK11	OK12
КЗ-1	+	+				+					+	+
КЗ-2		+							+		+	+
КЗ-3		+			+		+		+		+	+
КЗ-4			+			+					+	+
КЗ-5						+		+			+	+
КФ 1					+		+	+	+	+	+	+
КФ 2			+			+					+	+
КФ 3					+	+				+	+	+
КФ 4			+			+					+	+
КФ 5				+					+		+	+
КФ 6						+					+	+
КФ 7							+				+	+
КФ 8			+								+	+
КФ 9			+	+							+	+
КФ 10		+					+				+	+
КФ 11						+					+	+