

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ
Навчально-науковий інститут морського бізнесу
Кафедра кібербезпеки та захисту інформації

МЕТОДИЧНІ ВКАЗІВКИ
до освітнього компоненту
ОК 11 «Переддипломна практики»

другого (магістерського) рівня вищої освіти
галузі знань F Інформаційні технології
спеціальності F5 Кібербезпека та захист інформації
освітньо-професійна програма «Кібербезпека та захист інформації»

Методичні вказівки до освітньої компоненти ОК 11 **«Переддипломна практика»** для здобувачів другого (магістерського) рівня вищої освіти спеціальності F5 «Кібербезпека та захист інформації» денної та заочної форм навчання.

Методичні вказівки підготовлені співробітниками кафедри «Кібербезпека та захист інформації» Одеського національного морського університету: Кобозевою Аллою Анатоліївною, Лебедєвою Оленою Юріївною, Зоріло Вікторією Вікторівною з використанням в якості взірця:

Методичні вказівки для дисципліни «Проектно-технологічна практика» для спеціальності F3 «Комп'ютерні науки» денної та заочної форми навчання підготували викладачі кафедри «Кафедра технічної кібернетики й інформаційних технологій ім. проф. Р.В. Меркта» Одеського національного морського університету – доцент Романов Андрій Юрійович та доцент Даус Юрій Володимирович .

Методичні вказівки для освітньої компоненти «Переддипломна практика» схвалено кафедрою «Кібербезпека та захист інформації» ОНМУ (протокол №7 від 29.04.2026 р.)

Методичні вказівки для освітньої компоненти «Переддипломна практика» схвалено НМК ННПТІП (протокол №7 від 29.04.2026 р.)

ЗМІСТ

ЗМІСТ	3
ВСТУП.....	2
1 МЕТА І ЗАВДАННЯ ПРАКТИКИ	3
2 ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ТА РЕЗУЛЬТАТІВ НАВЧАННЯ, ЩО ЗАБЕЗПЕЧУЮТЬСЯ ПРАКТИКОЮ У ВІДПОВІДНОСТІ ДО ОСВІТНЬО- ПРОФЕСІЙНОЇ ПРОГРАМИ.....	4
3 ЗМІСТ ПРАКТИКИ.....	6
4 ІНДИВІДУАЛЬНІ ЗАВДАННЯ НА ПРАКТИКУ	7
5 МІСЦЯ ПРОВЕДЕННЯ ПРАКТИКИ.....	7
6. КАЛЕНДАРНИЙ ГРАФІК ПРОХОДЖЕННЯ ПРАКТИКИ.....	8
7 ВИМОГИ ЩОДО НАПИСАННЯ ТА ОФОРМЛЕННЯ ЗВІТУ ПРО ПРАКТИКУ	8
8 ПІДВЕДЕННЯ ПІДСУМКІВ ПРАКТИКИ ТА ОЦІНУВАННЯ ЗВІТУ	9
ДОДАТОК	11

ВСТУП

Переддипломна практика для студентів денної та заочної форми навчання другого (магістерського) рівня вищої освіти є одним із завершальних етапів підготовки до виконання магістерської кваліфікаційної роботи за спеціальністю F5 «Кібербезпека та захист інформації» за освітньо-професійною програмою «Кібербезпека та захист інформації» та входить до складу базових дисциплін. Вона становить важливу та обов'язкову ланку в підготовці висококваліфікованих спеціалістів до майбутньої діяльності за фахом, забезпечуючи їх відповідність зростаючим вимогам роботодавців та власну конкурентоспроможність на ринку праці.

Методичні вказівки складені відповідно до освітньо-професійної програми «Кібербезпека та захист інформації» підготовки здобувачів другого (магістерського) рівня вищої освіти за галуззю знань F «Інформаційні технології», спеціальності F5 «Кібербезпека та захист інформації» та Положення «Про проведення практики студентів вищих навчальних закладів України» від 08.04.93 р., розробленого Міністерством освіти України.

Методичні вказівки містять рекомендації щодо організації та проведення переддипломної практики здобувачів другого (магістерського) рівня вищої освіти. Наведено загальні положення щодо переддипломної практики, її мету, завдання та зміст, роз'яснення щодо оформлення звіту та питання підведення підсумків. Методичні вказівки спрямовані на допомогу студентам у питаннях планування, проведення та підведення підсумків практики.

Практична підготовка забезпечує закріплення теоретичних знань, а також набуття, вдосконалення і розширення професійних компетентностей, необхідних для успішної роботи за обраною спеціальністю. Програма практики покликана сприяти забезпеченню якісної теоретичної і практичної підготовки здобувачів другого (магістерського) рівня вищої освіти, опануванню фахових знань, умінь та навичок, формуванню організаторських та управлінських якостей, необхідних у майбутній професійній діяльності.

1 МЕТА І ЗАВДАННЯ ПРАКТИКИ

Метою практики є закріплення, поглиблення та систематизація теоретичних знань, отриманих під час навчання, а також набуття практичних навичок і професійних компетентностей із проєктування, розробки, розгортання та аудиту систем захисту інформації в соціокіберфізичних, комп'ютерних та телекомунікаційних системах. Практика спрямована на формування у майбутнього бакалавра здатності самостійно вирішувати інженерно-технічні, проєктні, організаційні завдання у сфері кібербезпеки відповідно до чинних стандартів та вимог нормативно-правових актів України.

Основні напрями переддипломної практики:

- Аналіз архітектури об'єкта захисту: дослідження структури інформаційно-комунікаційної системи бази практики або її критичних вузлів, наприклад, мереж БПЛА, серверних потужностей, баз даних;
- Проєктування елементів систем захисту: участь у розробці або модернізації комплексних систем захисту інформації, підборі засобів автентифікації, шифрування чи антивірусного захисту;
- Розробка профілів безпеки: формулювання моделей загроз та моделей порушника для конкретного технологічного процесу чи інформаційного ресурсу;
- Налаштування засобів кіберзахисту: практична робота з розгортання та конфігурування міжмережевих екранів (Firewalls), систем виявлення та запобігання вторгненням (IDS/IPS), систем моніторингу подій безпеки (SIEM);
- Управління вразливостями: проведення сканування мережі чи програмного забезпечення на наявність уразливостей за допомогою спеціалізованого інструментарію (наприклад, Nessus, Nmap, Burp Suite) та підготовка рекомендацій щодо їх усунення (пачінг, зміна конфігурацій);
- Реалізація криптографічних та стеганографічних методів: застосування на практиці алгоритмів шифрування, протоколів безпеки чи стеганографічних інструментів для прихованої і завадостійкої передачі даних або маркування контенту цифровими водяними знаками;
- Аудит та оцінка захищеності: участь в оцінюванні поточного рівня захищеності інформаційних ресурсів або об'єктів критичної інфраструктури організації;
- Аналіз кіберінцидентів (Елементи цифрової криміналістики): набуття навичок збору, аналізу та верифікації лог-файлів, виявлення аномальної активності або слідів несанкціонованого втручання в систему;
- Аналіз нормативно-правової бази: перевірка відповідності політик безпеки підприємства вимогам законодавства України;
- Розробка документації: участь у складанні технічних завдань на створення систем захисту, розробці інструкцій для користувачів та адміністраторів безпеки, формуванні внутрішніх політик ІБ;
- Командна взаємодія: набуття навичок роботи в команді для координації дій під час реагування на загрози.

Перелік завдань може бути доповнений та адаптований відповідно до профілю й специфіки обраної бази практики та індивідуального завдання на практику, але обов'язково повинен бути безпосередньо пов'язаним зі специфікою спеціальності F5 Кібербезпека та захист інформації.

2 ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ТА РЕЗУЛЬТАТІВ НАВЧАННЯ, ЩО ЗАБЕЗПЕЧУЮТЬСЯ ПРАКТИКОЮ У ВІДПОВІДНОСТІ ДО ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Інтегральна компетентність

Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки..

Загальні компетентності.

Компетентності, визначені стандартом вищої освіти спеціальності:

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.

Компетентності, визначені стандартом вищої освіти спеціальності:

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.

Програмні результати навчання

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.

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.

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.

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.

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 натурного, 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

3 ЗМІСТ ПРАКТИКИ

Переддипломна практика магістрів проводиться відповідно до освітньо-професійної програми в 3-му семестрі і триває 8 тижнів.

Керівництво практикою здобувача здійснюється керівником практики від університету та керівником практики від підприємства/установи – бази практики, та контролюється керівником магістерської кваліфікаційної роботи здобувача вищої освіти.

Зміст переддипломної практики визначається керівником магістерської кваліфікаційної роботи спільно зі здобувачем, узгоджується з керівником від підприємства у вигляді індивідуального завдання переддипломної практики.

Під час практики студент виконує індивідуальні завдання на практику згідно з календарним графіком її проходження, який затверджується керівником практики від підприємства. Практика має починатися зі знайомства з керівником того структурного підрозділу установи, в якому здобувач одержав робоче місце, а також з керівником практики від державної установи.

В результаті проходження переддипломної практики здобувач вищої освіти повинен:

- ознайомитись із підприємством, його організаційною структурою, підрозділом кібербезпеки, внутрішніми положеннями та політиками;
- зібрати і систематизувати інформацію, необхідну для магістерської кваліфікаційної роботи, що включає аналіз існуючих систем захисту, виявлення вразливостей, дослідження сучасних загроз і методів протидії;
- безпосередньо взяти участь у вирішенні реальних завдань, до яких може бути віднесено розробку політик безпеки, налаштування та адміністрування засобів захисту, проведення пентестів, розслідування інцидентів, розробку програмних модулів для підвищення безпеки;
- провести експерименти або моделювання для підтвердження гіпотез магістерської кваліфікаційної роботи;
- систематизувати отримані результати;
- скласти детальний звіт, подати та захистити його на кафедрі;

Опрацювання питань, передбачених індивідуальними завданнями на практику, слід починати з вивчення відомих нормативно-правових документів, які регламентують діяльність установи та відповідного структурного підрозділу, ознайомлення з посадовими інструкціями відповідних спеціалістів. Після цього головну увагу треба зосередити на вивченні робочих матеріалів установи, які розкривають зміст її діяльності. До таких матеріалів належать звіти, прогнози, плани, програми, аналітичні подання, методичні документи тощо, що не мають обмежень доступу. Інформація, яка міститься в названих

джерелах, є об'єктом цілеспрямованого аналізу та узагальнень. Її опрацювання слід підпорядковувати змісту індивідуальних завдань на практику у відповідності з компетентностями та результатами навчання, переліченими в розділі 2.

4 ІНДИВІДУАЛЬНІ ЗАВДАННЯ НА ПРАКТИКУ

Практика проводиться в індивідуальній формі. Індивідуальна форма – це безпосереднє вивчення кожним студентом програмних питань практики, написання відповідних програм.

Результати проходження практики студенти оформляють у вигляді письмового звіту про виконання індивідуальних завдань на практику, який подається на кафедру згідно з графіком організації навчального процесу. Зміст індивідуальних завдань на практику для кожного студента визначається керівником магістерської кваліфікаційної роботи. Індивідуальні завдання доводяться до відома кожного студента на початку практики. Завдання можуть редагуватися керівниками від бази практики, університету.

Завдання можуть бути пов'язані не тільки безпосередньо з діяльністю бази практики, а й з науково-дослідною роботою кафедри кібербезпеки та захисту інформації, якщо це не суперечить діяльності бази практики, підготовкою доповідей на наукову конференцію, написанням наукових статей та наукових робіт на конкурс. Науково-дослідна робота в період практики має бути спрямована на підвищення фахового рівня підготовки студентів.

5 МІСЦЯ ПРОВЕДЕННЯ ПРАКТИКИ

Розподіл студентів на практику проводить навчальний заклад - ОНМУ з урахуванням замовлень на підготовку фахівців. Вибір баз практики здійснює випускаюча кафедра з урахуванням завдань практики та можливістю їх реалізації. При цьому повинні враховуватись перспективи сучасних напрямків розвитку ІТ – галузі, економічного та соціального розвитку суспільства.

Студенти можуть самостійно з дозволу кафедри підбирати собі місце проходження практики і пропонувати його для використання, при цьому діяльність запропонованого студентом місця для практики повинна бути пов'язана зі спеціальністю F5 Кібербезпека та захист інформації. У цьому випадку організація на офіційному бланку надає лист-погодження прийняття студента на практику із зазначенням термінів проходження практики та назначенням керівника практики від підприємства. З такими базами практики ОНМУ завчасно укладає договір на її проведення.

Бази практики повинні бути профільними, забезпечувати можливість набуття здобувачем компетентностей та результатів навчання у відповідності с п.2.

Функції підприємства-бази практики:

- забезпечувати якісне проведення інструктажу з пожежної безпеки, охорони праці, кібербезпеки та промислової гігієни;
- надавати студентам місця практики, які забезпечують найбільшу ефективність її проведення;
- створювати необхідні умови для одержання студентами в період проходження практики знань за фахом;
- дотримувати календарного графіка проходження практики;
- надавати можливість студентам користуватися літературою, проєктною, техніко-економічною та іншою документацією, що не має обмежень доступу;
- надавати допомогу при відборі матеріалів для проведення проєктно технологічної практики;
- забезпечувати та контролювати дотримування студентами практикантами правил внутрішнього трудового розпорядку, які встановлені для конкретного підприємства.

Безпосереднє керівництво практикою покладається за наказом керівника підприємства на провідних спеціалістів структурних підрозділів.

6. КАЛЕНДАРНИЙ ГРАФІК ПРОХОДЖЕННЯ ПРАКТИКИ

Календарний графік проходження практики складається здобувачем разом з керівником практики. Один з можливих варіантів графіку наведений нижче.

Робочий день	Дата	Зміст виконаної роботи	Примітка
1		Прибуття на підприємство. Отримання перепустки (за необхідністю). Відмітка про прибуття на базу практики. Знайомство з основами техніки безпеки та охорони праці.	
2		Ознайомлення з робочим місцем та зі структурою підприємства/установи	
3-4		Складання плану магістерської кваліфікаційної роботи. Консультування з керівником практики, можливі корективи завдання (консультування з викладачами кафедри кібербезпеки та захисту інформації).	
5		Узгодження етапів розробки, завдання та термінів реалізації з керівником практики.	
6-11		Підбір літературних джерел за темою дослідження.	
12-35		Проведення досліджень за темою магістерської кваліфікаційної роботи.	
36-40		Підготовка звітної документації. Оформлення пояснювальної записки до звіту, підготовка графічного матеріалу (діаграм, скріншотів). Отримання відгуку та оцінки від керівника бази практики.	
40		Вибуття з підприємства. Відмітка про вибуття з бази практики	
		Здача та захист звіту з практики в університеті	

7 ВИМОГИ ЩОДО НАПИСАННЯ ТА ОФОРМЛЕННЯ ЗВІТУ ПРО ПРАКТИКУ

Звіт з проходження практики – це основний підсумковий документ, що надає можливість проаналізувати і оцінити діяльність здобувача під час проходження практики. Звіт, що відображає результати виконання завдань програми, має бути складений за час проходження практики.

Текстова частина звіту, як правило, супроводжується рисунками, схемами, фотографіями, ескізами, бланками технічної документації тощо. Обсяг звіту з переддипломної практики, включаючи ілюстрації, становить 20 – 40 сторінок.

Текст має бути набраний на комп'ютері на одному боці стандартного аркуша формату А4. Поля на кожній сторінці мають бути такі: верхній, нижній, лівий 25 мм, правий 10 мм. Нумерація сторінок — наскрізна: перша сторінка — титульний аркуш, але

на ньому номер сторінки не ставиться. Усі ілюстрації звіту нумеруються послідовно арабськими цифрами. Кожну ілюстрацію треба супроводжувати коротким аналізом її змісту та висновками.

Звіт із переддипломної практики має відповідати вимогам до звітів НДР / ДСТУ 3008-95 Державний стандарт України. Документація. Звіти в сфері науки і техніки. Структура і правила оформлення.

Звіти здобувачів вищої освіти, які не виконали програму практики або отримали незадовільну характеристику про роботу на кафедрі під час практики, оцінюються незадовільно.

До звіту входять:

- Титульний аркуш (див. додаток А);
- Зміст, де наводяться назви всіх розділів звіту;
- Вступ – описується актуальність та новизну роботи, її місце в сучасних дослідженнях, визначення мети та завдання практики (1 - 2 сторінки);
- Основна частина, в якій подаються відповіді на питання, передбачені індивідуальними завданнями на практику. Вміст та наповненість цієї частини звіту залежить від теми кваліфікаційної роботи. Як правило, основна частина звіту може складатися з двох частин. У першій частині проводиться вибір технічного рішення на основі реферативного огляду літератури за темою роботи, який повинен вміщувати в себе аналіз технічних та наукових джерел. У цьому розділі розглядаються питання призначення та основні параметри об'єкту проектування, проводиться аналітичний огляд існуючих та перспективних рішень. У другій частині проводиться порівняльний аналіз відомих технічних рішень;
- Висновки – в цьому розділі наводиться загальний огляд одержаних результатів та їх порівняння з аналогами; пропозиції та рекомендації щодо використання одержаних результатів або необхідність додаткових або паралельних досліджень;
- Список використаних джерел – може включати наукові роботи, статті, дисертації, періодичні видання, підручники, закони і законопроекти. Список використаних джерел складається відповідно до ДСТУ 7.1:2006.

Правильно оформлений звіт подається на кафедру згідно з графіком організації навчального процесу.

8 ПІДВЕДЕННЯ ПІДСУМКІВ ПРАКТИКИ ТА ОЦІНЮВАННЯ ЗВІТУ

Підсумки

Оформлений звіт студент у встановлений термін подає на кафедру для перевірки керівником магістерської кваліфікаційної роботи. Керівник кваліфікаційної роботи у своєму висновку відображає рівень засвоєних студентом теоретичних знань та умінь застосовувати їх на практиці, відомості про виконання студентом усіх розділів програми практики, якість оформлення звітної документації, висновки та попередню оцінку проходження практики студентом – з урахуванням характеристики і оцінки, наданої керівником практики від підприємства.

У випадку наявності суттєвих відхилень від вимог до змісту й оформлення, звіт повертається студенту на доопрацювання. Якщо звіт відповідає всім вимогам, він допускається до захисту. Захист звіту приймає комісія у складі викладачів, призначених завідуючим кафедрою. Кожен студент має усно захищати звіт про проходження навчальної практики.

Під час захисту визначається якість виконання робочої програми, глибина знань з висвітлених питань, рівень оволодіння студентом практичними навичками самостійної

роботи зі спеціальності.

За результатами захисту виставляється диференційована оцінка, яка фіксується на титульному аркуші, у відомості.

Результати захисту звітів за підсумками навчальної практики та висновки оформлюються протоколом та заносяться до відомостей, які передаються в навчальну частину університету.

Оцінювання звіту про проходження практики

Попередня оцінка виставляється за результатами перевірки керівником кваліфікаційної роботи звіту про проходження навчальної практики. Остаточна оцінка за навчальну практику виставляється керівником від кафедри за результатами захисту. Під час захисту студент повинен показати здобуті знання і вміння, застосовувати їх під час відповіді на запитання.

Звіт про проходження навчальної практики оцінюється за 100-бальною шкалою. Критерії оцінювання підсумкового контролю визначаються відповідно до Положення про організацію освітнього процесу Одеського національного морського університету та з урахуванням специфіки освітнього компонента (навчальної дисципліни).

- 100-90/ A/ відмінно – здобувач освіти має глибокі і системні знання, вміє узагальнювати матеріал, співвідносити загальні знання з конкретними ситуаціями; засвідчив уміння критично оцінювати варіантні підходи щодо сутності норм та уявлень; оволодів навичками аналізувати, моделювати та оцінювати ситуацію; обізнаний з науковими працями вітчизняних та зарубіжних фахівців в даній області; матеріал викладає логічно, послідовно, впевнено;
- 89-74/ B,C/ добре – здобувач освіти виявив достатньо повні знання курсу освітнього компонента; дає правильні, хоча і не завжди повні визначення; оволодів навичками співвідносити теоретичні знання з конкретними ситуаціями; висловлює своє ставлення до варіантних теорій щодо сутності явищ; засвоїв основи аналітичного методу; допускає незначні неточності в розкритті окремих положень;
- 73-60/ D,E/ задовільно – здобувач освіти поверхнево опанував матеріал освітнього компонента, володіє основними положеннями на мінімально допустимому рівні; може висловити своє ставлення до проблемних питань, не повною мірою обґрунтовано; вміє аналізувати набуті теоретичні знання і співвідносити їх з конкретними ситуаціями; виклад матеріалу непослідовний та неточний;
- 59-1/ F/ незадовільно – здобувач освіти виявив слабкі знання матеріалу освітнього компонента або їх відсутність; не зміг дати визначення основних категорій та термінів; відсутні навички оцінки норм і теорій; виклад матеріалу непослідовний, нелогічний та фрагментарний.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

Василько Василь Васильович.

3BIT

з переддипломної практики

Спеціальність: F5 Кібербезпека та захист інформації

Освітня програма: Кібербезпека та захист інформації

Керівник від Одеського національного
морського університету

О.Ю.Лебедева, к.т.н, доцент

(підпис)

<< >>

20_p

Керівник від (назва підприємства,
організації, установи)

(прізвище та ініціали)

(підпис)

<< >>

20_p