

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут інформаційних технологій та інноваційного
підприємництва

Кафедра кібербезпеки та захисту інформації

МЕТОДИЧНІ ВКАЗІВКИ

для освітньої компоненти

«ВИРОБНИЧА ПРАКТИКА»

для здобувачів
першого (бакалаврського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації
галузі знань F Інформаційні технології

Методичні вказівки для освітньої компоненти «Виробнича практика» для спеціальності F5 Кібербезпека та захист інформації денної та заочної форми навчання підготовлені співробітниками кафедри «Кібербезпека та захист інформації» Одеського національного морського університету: Кобозєвою 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 схвалено на засіданні кафедри «Кібербезпека та захист інформації» (Протокол від «29» квітня 2026 р. № 7)

Методичні вказівки схвалено на засіданні НМК ННІ ІТІП (Протокол від «29» квітня 2026 р. № 7)

ЗМІСТ

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	6
5 Місця проведення практики	7
6 Календарний графік проходження практики	8
7 Вимоги щодо написання та оформлення звіту про практику	9
8 Підведення підсумків практики та оцінювання звіту	10
Додаток. Зразок оформлення титульної сторінки звіту	12

ВСТУП

Програму практики складено відповідно до освітньо-професійної програми підготовки студентів за галуззю знань F Інформаційні технології, спеціальності F5 Кібербезпека та захист інформації першого (бакалаврського) освітньо-кваліфікаційного рівня.

Методичні вказівки складені у відповідності з діючим Положенням «Про проведення практики студентів вищих навчальних закладів України» від 08.04.93 р., розробленим Міністерством освіти України.

Виробнича практика є обов'язковим компонентом підготовки фахівців першого (бакалаврського) освітньо-кваліфікаційного рівня спеціальності F5 Кібербезпека та захист інформації. Вона передбачає безперервність та послідовність її проведення, одержання необхідного обсягу знань і умінь відповідно до Стандарту освіти. Програма практики покликана сприяти забезпеченню якісної теоретичної і практичної підготовки бакалаврів, 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 проектування, 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, проектні, організаційні завдання у сфері кібербезпеки відповідно до чинних стандартів та вимог нормативно-правових актів України.

Основні завдання практики:

- Аналіз архітектури об'єкта захисту: дослідження структури інформаційно-комунікаційної системи бази практики або її критичних вузлів, наприклад, мереж БПЛА, серверних потужностей, баз даних;
- Проектування 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, але обов'язково повинен бути безпосередньо пов'язаним зі специфікою спеціальності F5 Кібербезпека та захист інформації.

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

Інтегральна компетентність

Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

Загальні компетентності

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.

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.

Спеціальні компетентності

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.

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.

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.

Програмні результати навчання

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

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.

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.

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

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.

3 ЗМІСТ 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 студент одержав робоче місце, а також з керівником практики від державної установи. 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 залежить від специфіки діяльності конкретної установи (бази практики). 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

День	Дата	Зміст виконаної роботи	Години	Примітка
1		Установча конференція. Знайомство з програмою та методичними рекомендаціями щодо проходження та оформлення практики. Відмітка про прибуття на базу практики. Знайомство з основами техніки безпеки та охорони праці.	8	
2		Поділ на команди, розподіл функціональних ролей та визначення цілей майбутньої практики. Опис посадових обов'язків на базі практики	8	
3-5		Розробка технічного завдання. Узгодження етапів розробки та термінів реалізації з керівником практики.	24	
6-22		Виконання технічного завдання, консультування з керівником практики, можливі корективи завдання (консультування з викладачами кафедри кібербезпеки та захисту інформації).	136	
23-25		Підготовка звітної документації. Оформлення пояснювальної записки до звіту, підготовка графічного матеріалу (діаграм, скріншотів). Отримання відгуку та оцінки від керівника бази практики. Пропозиції та висновки щодо поліпшення стану проходження технологічної практики.	24	

7 ВИМОГИ ЩОДО НАПИСАННЯ ТА ОФОРМЛЕННЯ ЗВІТУ ПРО ПРАКТИКУ

До звіту входять:

- титульний аркуш (див. додаток А);
- зміст, де наводяться назви всіх розділів звіту;
- основна частина, в якій подаються відповіді на питання, передбачені індивідуальними завданнями на практику.

Обсяг звіту — 15 - 20 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 з практики має наступну типову структуру:

1. Вступ – визначення мети та завдання практики (1 сторінка).
2. Основна частина (до 12 сторінок) виконання індивідуального завдання на практику), яке охоплює:
 - 2.1. Загальна характеристика установи (до 3 сторінок), зокрема:
 - основних нормативно-правових документів, які регламентують її діяльність і не мають обмежень доступу;
 - організаційно-управлінської структури, зв'язків з іншими органами, підприємствами та організаціями;
 - завдань та функціональних обов'язків спеціалістів підрозділу;
 - обов'язків та прав службовців підрозділу (провідного спеціаліста, головного спеціаліста) відповідно до посадових інструкцій).
 - 2.2. Характеристику сфери діяльності установи (в межах компетенцій відповідного структурного підрозділу (управління, відділу), яка включає (до 2 сторінок).
 - 2.3. Пропозиції щодо вдосконалення процесу застосування інформаційних технологій в межах бази практики (до 3 сторінок).
 - 2.4. Результати виконання індивідуального завдання студентом, які передбачають розкриття:
 - набутих професійних знань в результаті особистої участі студента у заходах, що проводяться установою;
 - отриманих практичних вмінь від участі студента у оновленні комп'ютерних баз даних, збору та систематизації різних інформаційних документів, якими оперує в своїй діяльності установа, практичних вмінь обробки, зберігання, захисту інформації тощо;
 - компетенцій, що були отримані студентом під час практики.
3. Висновки (щодо набутих студентом вмінь та навичок під час проходження практики (1 сторінка)).
4. Список використаних джерел.

5. Додатки (виконане особисто студентом завдання за дорученням керівника від бази практики, нормативно-правові документи (за необхідності) тощо).

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

8 ПІДВЕДЕННЯ ПІДСУМКІВ ПРАКТИКИ ТА ОЦІНУВАННЯ ЗВІТУ

Підсумки

Оформлений звіт студент у встановлений термін подає на кафедру для перевірки керівником практики від кафедри. Керівник практики від кафедри 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 від кафедри звіту про проходження навчальної практики. Остаточна оцінка за навчальну практику виставляється 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/ А/ 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.

ДОДАТОК**ЗРАЗОК ОФОРМЛЕННЯ ТИТУЛЬНОЇ СТОРІНКИ ЗВІТУ**

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

Василько Василь Васильович,

студент групи _____

ЗВІТ

з виробничої практики

Спеціальність: F5 Кібербезпека та захист інформації
Освітня програма: Кібербезпека та захист інформації

Керівник від Одеського національного
морського університету

О.Ю.Лебедева, канд.техн.наук, доцент

«_____» _____ 20__р
(підпис)

Керівник від (назва підприємства,
організації, установи)

_____ (прізвище та ініціали)

«_____» _____ 20__р
(підпис)

Одеса – 20____