МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерної інженерії та інноваційних технологій

«ЗАТВЕРДЖУЮ»

Ректор Міжнародного гуманітарного університету д.ю.н., професор

_____ Костянтин ГРОМОВЕНКО

«____» _____ 2023 р.

РОБОЧА ПРОГРАМА ПЕРЕДДИПЛОМНОЇ ПРАКТИКИ

Галузь знань 12 – «Інформаційні технології»

Спеціальність 125 – «Кібербезпека та захист інформації»

Назва освітньої програми Кібербезпека

Рівень вищої освіти другий (магістерський) рівень

Одеса -- 2023 рік

Робоча програма затверджена на засіданні кафедри комп'ютерної інженерії та інноваційних технологій протокол № 1 від 1 вересня 2023 року.

Розробник і викладач	**Контактний тел.**	**E-mail**
Викладач кафедри комп'ютерної інженерії та інноваційних технологій **Швець Оксана Володимирівна**	0673051784	ovshvets@ukr.net

Завідувач кафедри комп'ютерної інженерії та інноваційних технологій к.т.н., доцент _____ Лариса ЙОНА

Гарант освітньої програми _____ Лариса ЙОНА

Узгоджено
Начальник навчального відділу _____ Лариса РАЙЧЕВА

1. МЕТА І ЗАВДАННЯ ПРАКТИКИ

Переддипломна практика є складовою частиною навчального процесу у підготовці фахівців зі спеціальності 125 – «Кібербезпека та захист інформації», а також обов'язковим компонентом освітньої програми для здобуття освітнього рівня «магістр». Переддипломна практика проводиться у третьому семестрі. Вона передбачає удосконалення професійно-практичної підготовки здобувачів та забезпечує набуття ними визначених освітньою програмою компетентностей з використанням матеріально-технічної бази практики. Переддипломна практика є завершальним етапом навчання та передує виконанню здобувачами вищої освіти кваліфікаційної роботи. Вона передбачає узагальнення й удосконалення здобутих ними знань, практичних умінь і навичок, оволодіння професійним досвідом з метою їх підготовки до самостійної трудової діяльності, а також збір матеріалів для виконання кваліфікаційних робіт.

Метою переддипломної практики є самостійне практичне освоєння здобувачами сукупності прийомів і методів дослідження для розв'язання конкретних задач, а також придбання професійного досвіду.

Головним завданням переддипломної практики є збір матеріалів для виконання кваліфікаційної роботи. Матеріали, зібрані під час перебування на практиці, мають бути вихідними даними для розробки кваліфікаційної роботи. Необхідні матеріали здобувач одержує, відвідуючи відповідні відділи організацій (підприємств).

Строки проведення практики та обсяг годин визначається навчальним планом. Порядок проходження практики встановлюється статтею 51 Закону України «Про вищу освіту», «Положенням про проведення практики студентів вищих навчальних закладів України», затвердженим наказом Міністерства освіти України № 93 від 08.04.1993.

Відповідно до вимог освітньо-професійної програми здобувачі вищої освіти повинні набути наступних компетентностей:

Інтегральна компетентність (ІК)	
ІК	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-3	Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові 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.

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.
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.
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.
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	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
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.
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.
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.

2. ОРГАНІЗАЦІЯ, ПРОВЕДЕННЯ І КЕРІВНИЦТВО ПРАКТИКОЮ

В організації та проведенні практики керівники практики і здобувачі керуються нормами та визначеними нормативно-правовими актами:

– Закон України «Про вищу освіту» від 1 липня 2014 року;

– Положення про проведення практики студентів вищих навчальних закладів України, затверджене наказом Міністерства освіти України від 8 квітня 1993 р. № 93;

– Положення про практичну підготовку здобувачів Міжнародного гуманітарного університету.

2.1 Організація та проведення практики

Загальна організація, проведення і контроль практики покладається на відповідального за практику на факультеті кібербезпеки програмної інженерії та комп'ютерних наук. Навчально-методичне керівництво і виконання програми практики забезпечується кафедрою комп'ютерної інженерії та інноваційних технологій.

У процесі проходження здобувач заповнює щоденник, в якому наводяться відомості про здобувача, назва бази практики, вид практики, період проходження практики, календарний графік із переліком робіт, запланованих до виконання.

Протягом перших трьох днів здобувач на базі практики повинен пройти інструктаж з техніки безпеки. У період проходження практики здобувачі дотримуються всіх правил внутрішнього розпорядку і техніки безпеки, встановлених в підрозділі і на робочих місцях.

До завершення практики здобувачеві необхідно:

– заповнити щоденник практики та отримати відгук керівника від бази практики.

– оформити звіт з практики, титульний аркуш якого підписується здобувачем вищої освіти та керівником від університету

Практична підготовка здобувачів, які навчаються за дистанційною формою навчання, проводиться із використанням технологій дистанційного навчання за наявності відповідних веб-ресурсів і можливостей доступу до них.

Керівник практики від факультету кібербезпеки, програмної інженерії та комп'ютерних наук здійснює методичне керівництво практикою, надає здобувачам допомогу у виконанні програми практики, веденні щоденника, складання звіту про проходження практики, бере участь у роботі комісії під час захисту практики, підбиває підсумки і виставляє оцінку, враховуючи характеристику, одержану здобувачем за місцем проходження практики, зміст звіту і результати його захисту.

Безпосередньо проходженням практики здобувачами керує працівник підприємства, на якому проходить практику здобувачі, призначений керівництвом. Всі зауваження щодо дисципліни здобувача заносяться керівником у щоденник.

Після закінчення практики здобувачі надають керівнику практики від факультету кібербезпеки, програмної інженерії та комп'ютерних наук щоденник та звіт з проходження практики.

Щоденник практики заповнюється здобувачем та містить відгук керівника від бази практики, який засвідчується підписом керівника підприємства та мокрою печаткою бази практики (підприємства). Відгук керівника від бази практики повинен відображати ділові та моральні якості, виявлені здобувачем під час проходження практики, та містити рекомендовану оцінку його діяльності.

Після закінчення практики належним чином оформлений щоденник разом із звітом повинен бути перевірений керівниками практики, які складають відгуки і підписують його.

Захист результатів практики здійснюється впродовж перших десяти днів семестру, що починається після практики, або протягом перших десяти днів після її закінчення.

Здобувачеві вищої освіти, який не виконав програму практики без поважних причин, може бути надано право проходження практики повторно при виконаних умов, визначених навчальним закладом. Здобувач вищої освіти, який при захисті практики отримав негативну оцінку, відраховується з закладу вищої освіти.

2.2 Вимоги до бази практики

Практика здобувачів вищої освіти університету проводиться в установах, які відповідають меті, завданням, змісту практики, а також вимогам освітніх програм.

Базами проведення практики можуть бути навчальні, виробничі й наукові підрозділи Університету чи іншого закладу вищої освіти, інститути НАН України, підприємства, організації, установи різних галузей економіки Україні та за її межами, які мають належні умови для проведення практики та відповідають профілю освітньої програми.

Перелік рекомендованих баз практик
для магістрів факультету Кібербезпеки, програмної інженерії та комп'ютерних наук, що навчаються за спеціальністю 125 – Кібербезпека та захист інформації

	Підприємство	**Дата та номер договору із Міжнародним гуманітарним університетом**
1	Освітній фонд «Кіпсолід»	Договір №040 від 16.11.2022
2	Управління протидії кіберзлочинам в Одеській області Департаменту кіберполіції Національної поліції України	Договір №044 від 18.11.2022
3	ТОВ «Альфа ТВ»	Договір №042 від 02.11.2022
4	ТОВ «ЕЛАН-ІНЕТ»	Договір №041 від 7.11.2022
5	ТОВ «Телекарт-Прилад»	Договір №4554 від 2.09.2022
6	ТОВ «РЕНОМЕ СЕРВІС»	Договір №039 від 1.11.2022
7	ТОВ «Гігабайт+»	Договір №043 від 10.11.2022
8	ТОВ «Телекомунікаційні технології»	Договір №047 від 29.11.2022
9	ДП "Одеський науково-дослідний інститут зв'язку"	Договір №093 від 23.12.2022
10	ТОВ «Люксофт солюшнс»	Договір №SC-MSA-095748 від 14.08.2023
11	ТОВ «Компарус.юа»	Договір №16/1 від 20.07.2023
12	ТОВ «Мегабіт СЛ»	Договір №4560 від 18.11.2022
13	Громадська спілка «Айті Фемелі Одеса»	Договір №17/1 від 20.07.2023
14	Громадська організація «Асоціація Ноосфера»	Договір №7 від 23.06.2023
15	Спілка об'єднань громадян «Об'єднання організацій роботодавців Одеської області»	Договір №8 від 06.04.2023

Визначення баз практики здійснюється кафедрою комп'ютерної інженерії та інноваційних технологій на основі відповідних договорів із підприємствами, організаціями, установами, незалежно від їх організаційно-правових форм і форм власності.

У разі підготовки фахівців за цільовими договорами, базами практики є підприємства, організації та установи, для яких здійснюється така підготовка.

Здобувачі вищої освіти за погодженням з кафедрою комп'ютерної інженерії та інноваційних технологій можуть самостійно обирати місце її проходження і пропонувати для укладання відповідні договори.

Здобувачі вищої освіти можуть проходити практику за межами України в порядку, встановленому чинним законодавством і договорами про співпрацю, укладеними Університетом з іншими закладами вищої освіти, науковими установами тощо інших держав.

2.3 Обов'язки керівника практики від факультету кібербезпеки, програмної інженерії та комп'ютерних наук

Керівник практики від факультету кібербезпеки, програмної інженерії та комп'ютерних наук:

– до початку практики знайомиться з базами практики і організовує належні умови для проходження практики;

– забезпечує проведення всіх організаційних заходів перед початком практики й інструктажу з практики та техніки безпеки, організує вручення здобувачам необхідні документи з практики (програму практики та щоденник);

– повідомляє здобувачам про систему звітності з практики, запроваджену на факультеті кібербезпеки, програмної інженерії та комп'ютерних наук, а саме: оформлення щоденника та звіту;

– організує явку здобувачів на практику, регулярно контролює відвідування занять, спостерігає за ходом занять і виконанням програми і тематичного плану практики;

– надає необхідну навчально-методичну допомогу здобувачам та представникам підприємства, що залучені до проведення занять;

– перевіряє правильність ведення щоденника практики та виконання завдань;

– контролює забезпечення нормальних умов праці і побуту здобувачів та проведення з ними обов'язкових інструктажів з охорони праці і техніки безпеки;

– контролює виконання здобувачами правил внутрішнього трудового розпорядку, доповідає декану факультету кібербезпеки, програмної інженерії та комп'ютерних наук про порушення трудової дисципліни.

2.4 Обов'язки керівника практики від бази практики

Керівник практики від бази практики (підприємства, організації, тощо):

– приймає здобувачів на практику згідно з календарним планом;

– забезпечує проведення всіх організаційних заходів перед початком практики й інструктажу з практики та техніки безпеки;

– призначає наказом кваліфікованих спеціалістів для безпосереднього керівництва практикою;

– створює необхідні умови для виконання здобувачами програми практики, не допустити використання їх на посадах і роботах, що не відповідають програмі практики та майбутній спеціальності;

– забезпечує здобувачам умови безпечної роботи на кожному робочому місці;

– надає здобувачам і керівнику практики від факультету кібербезпеки, програмної інженерії та комп'ютерних наук можливість ознайомитися з нормативними актами та службовою документацією, необхідною для виконання програми практики;

– повідомляє керівника практики від факультету кібербезпеки, програмної інженерії та комп'ютерних наук та безпосередньо декана факультету про всі порушення трудової дисципліни, внутрішнього розпорядку практикантами та про інші порушення;

– допомагає здобувачам оволодіти програмним матеріалом, отримати всі необхідні навички та досвід роботи на підприємстві.

2.5 Обов'язки здобувача

Здобувач зобов'язаний:

– отримати від керівника практики факультету кібербезпеки, програмної інженерії та комп'ютерних наук консультації щодо оформлення всіх необхідних документів (програми практики та щоденника)

– пройти інструктаж про порядок проходження практики та підприємстві;

– пройти інструктаж з техніки безпеки;

– своєчасно прибути на базу практики;

– у повному обсязі виконувати всі завдання, передбачені програмою практики і вказівками її керівників;

– вивчити і суворо дотримуватись правил охорони праці і безпеки;

– систематично вести щоденник за встановленою формою;

– вивчити і дотримуватись діючих в організації правил внутрішнього розпорядку і трудової дисципліни;

– своєчасно підготувати звіт та скласти залік з практики.

Під час проходження практики здобувач повинен дотримуватись правил техніки безпеки та внутрішнього розпорядку, що діють на базі практики. Режим роботи, встановлений для працівників бази практики, є обов'язковим для здобувачів, які проходять практику. За порушення трудової дисципліни і правил внутрішнього трудового розпорядку здобувач несе дисциплінарну відповідальність перед адміністрацією бази практики.

3 ПОРЯДОК ПІДВЕДЕННЯ ПІДСУМКІВ ПРАКТИКИ ТА ОФОРМЛЕННЯ ЗВІТНИХ МАТЕРІАЛІВ

3.1 Вимоги до оформлення звіту з практики

Оформлення звіту повинно відповідати ДСТУ 3008-95 Документація. Звіти в сфері науки і техніки. Структура і правила оформлення.

Звіт складається з:

– титульного аркушу;

– змісту, який містить назви всіх розділів із зазначенням сторінок, на яких вони викладені;

– вступу, у якому зазначено мету та зміст практики;

– основної частини, у якому визначена суть завдання;

– висновків;

– списку використаних джерел;

– додатків.

Звіт повинен мати естетичний вигляд. Рекомендовано сторінки звіту скріплювати за допомогою «папки-планки». Рекомендований обсяг звіту – 10…15 аркушів.

Усі елементи звіту, у тому числі рисунки та таблиці, повинні бути написані державною мовою. Винятком, у яких дозволяється використовувати іншомовні слова, є копії екрану та фотографії.

3.2 Критерії оцінки результатів проходження практики

Практика оцінюється на «відмінно» (90-100 балів), якщо її результати повністю відповідають завданню практики, матеріал звіту повністю розкриває поставлене завдання. При

цьому зві. Відмінна оцінка визначає високий рівень самостійності при виконанні звіту, грамотність написання та охайність оформлення, вчасність подання звіту керівнику практики.

Звіт оцінюється на «добре» (74-89 балів) за наявності незначних недоліків (звіт містить не менше 75% викладеного розв'язання поставленого завдання), недостатності точних висновків, поодиноких випадків порушення логіки викладу матеріалу та вимог стилю, перевантаженості непотрібною інформацією, огріхами в оформленні звіту.

За наявності значних недоліків (звіт містить не менше 60% викладеного розв'язання поставленого завдання), неправильно розроблено програму або виконання завдання поверхово, не витримано вимог до оформлення звіту тощо — керівник практики оцінює звіт на «задовільно» (60-73 бали).

Якщо звіт з практики не задовольняє зазначених вимог (зміст не відповідає поставленому завданню, відсутній звіт написано неграмотно та неохайно оформлено тощо і містить менше 60% викладеного розв'язання поставленого завдання) — керівник практики оцінює звіт на «незадовільно» (0-59 балів).

Таблиця відповідності результатів контролю знань за різними шкалами

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	Зараховано
74-81	C		
64-73	D	Задовільно	Зараховано
60-63	E		
35-59	Fx	Незадовільно	Не зараховано
1-34	F		

4. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Про вищу освіту: Закон України від 01.07.2014. Відомості Верховної Ради України. 2014. № 37-38. Ст. 2004.
2. ДСТУ 3008:2015 Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Введ. 01.07.2017. - Київ: Держстандарт України, 2016. – 31 с.
3. ДСТУ 3582:2013 Інформація та документація. Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила- Введ. 01.01.2014. - Київ: Держстандарт України, 2014. – 17 с.
4. ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання - Введ.01.07.2016. - Київ: Держстандарт України, 2016. – 20 с.
5. «Положення про практичну підготовку здобувачів Міжнародного гуманітарного університету», МГУ, 2022.
6. Державний стандарт України Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
7. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
8. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
9. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.

10. НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.

11. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

12. НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення.

13. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

14. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

15. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

16. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

17. НД ТЗІ 2.7-011-12 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв.

18. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи.

19. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

20. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

21. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

Інформаційні ресурси

22. Національна бібліотека України ім. В.І. Вернадського. URL: http://www.nbuv.gov.ua.

23. Он-лайн бібліотека. URL: http://www.lib.com.ua.

24. Портал штучного інтелекту. URL: https://openai.com/