



Міжнародний гуманітарний університет
Факультет кібербезпеки, програмної інженерії
та комп'ютерних наук
Кафедра комп'ютерних наук

«ЗАТВЕРДЖУЮ»

Ректор Міжнародного
гуманітарного університету

д.ю.н., професор

Костянтин ГРОМОВЕНКО

сергій 2025 р.



РОБОЧА ПРОГРАМА НАСКРІЗНОЇ ПРАКТИКИ

Галузь знань

12 «Інформаційні технології»

Спеціальність

125 – «Кібербезпека та захист інформації»

Назва освітньої програми

«Кібербезпека»

Рівень вищої освіти

перший (бакалаврський)

Одеса – 2025 рік

Робоча програма затверджена на засіданні кафедри Комп'ютерної інженерії та інноваційних технологій

Протокол № 1 від 28 серпня 2025 року.

Розробники і викладачі	Контактний тел.	E-mail
доцент кафедри інформаційних технологій, кандидат технічних наук Григор'єва Тетяна Ігорівна	+380679075695	t.grygoryeva@mgu.edu.ua

Завідувач кафедри Комп'ютерної інженерії та інноваційних технологій

к.т.н., доцент

 Лариса Йона

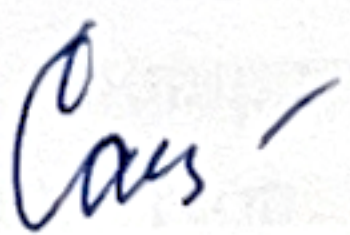
Гарант освітньої програми

к.т.н., доцент

 Лариса Йона

Узгоджено

Начальник навчального відділу

 Лілія САЄНКО

1 ПОЯСНЮВАЛЬНА ЗАПИСКА

Наскрізна програма практики складена відповідно до освітньо-професійної програми «Кібербезпека» підготовки здобувачів першого (бакалаврського) рівня вищої освіти зі спеціальності 125 Кібербезпека та захист інформації. Практика є обов'язковою складовою частиною процесу підготовки здобувачів першого (бакалаврського) рівня вищої освіти і передбачає безперервність та послідовність її проведення з метою одержання необхідного рівня теоретичних знань, формування професійних вмінь і навичок, відповідно до стандартів освіти. Наскрізна програма практики є розгорнутим планом професійної підготовки майбутніх фахівців зі спеціальності 125 Кібербезпека та захист інформації з врахуванням їхнього теоретичного та практичного навчання. Вона визначає основні аспекти проведення практик, їх системність, послідовність та забезпечує єдиний комплексний підхід до організації та проведення практик.

Наскрізна програма практики для першого (бакалаврського) рівня вищої освіти містить чотири курси з практичного навчання здобувачів: «Навчальна практика», «Технологічна практика», «Виробнича практика» та «Переддипломна практика». Всі вони належать до переліку обов'язкових освітніх компонент освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації.

Порядок проходження практики встановлюється наступними нормативними документами:

- Законом України «Про фахову передвищу освіту» від 6 червня 2019 року;
- Положенням про проведення практики студентів вищих навчальних закладів України, затвердженим наказом Міністерства освіти України №93 від 08.04.1993;
- Положенням про практичну підготовку здобувачів вищої та фахової передвищої освіти Міжнародного гуманітарного університету, затвердженим Вченою радою Міжнародного гуманітарного університету 6 липня 2023 року (протокол №7).

2 ОСНОВНІ ПОЛОЖЕННЯ

2.1 Місце практик в професійній підготовці здобувача

Усі види практики повинні збагатити та поширити загальну професійну підготовку здобувачів та активно сприяти формуванню теоретичних та практичних навичок майбутнього спеціаліста, його професійних та виробничих навиків, його ознайомлення з сучасними технологічними та професійними процесами виробництва, а також допомогти написанню кваліфікаційної роботи.

Дисципліни пов'язані з наступними фундаментальними та професійно-орієнтованими дисциплінами освітньо-професійної програми «Кібербезпека» - «Криптографія та криптоаналіз», «Теорія інформації та кодування», «Програмування та захист ігрових застосунків», «Комплексні системи захисту інформації» та іншими загальноосвітніми дисциплінами.

2.2 Мета практик

Оволодіння здобувачами вищої освіти сучасними технологіями та формами організації праці у сфері їхньої майбутньої професії, формування у них, на базі одержаних під час навчання в університеті теоретичних знань та практичної підготовки, професійних умінь і навичок для прийняття самостійних рішень у процесі їхньої професійної діяльності; формування здатності систематично поновлювати свої знання та творчо застосовувати їх у практичній діяльності у сфері кібербезпеки та захисту інформації.

2.3 Завдання практик

Головним завданням практик є створення основи для майбутньої професійної діяльності, практичних знань, вмінь і навичок, та особистих якостей майбутнього фахівця в галузях кібербезпеки та захисту інформації.

2.4 Характеристики практик

2.4.1 Навчальна практика

Навчальна практика студентів Факультету кібербезпеки, програмної інженерії та комп'ютерних наук Міжнародного гуманітарного університету є невід'ємною складовою підготовки фахівців та обов'язковою освітньою компонентою освітньої програми підготовки за першим (бакалаврським) рівнем, що має на меті набуття студентами професійних навичок і вмінь.

Навчальна практика приділяє увагу:

- поглибленню і закріпленню теоретичних знань, одержаних при вивченні дисциплін навчального плану спеціальності 125 Кібербезпека та захист інформації
- ознайомлення сучасними методами, формами організації праці в галузі майбутньої професії;
- навчанню самостійності у вирішенні певних питань та прийнятті рішень;
- набуттю навичок розв'язання реальних завдань, використовуючи отримані знання.

Згідно з навчальним планом спеціальності 125 Кібербезпека та захист інформації Факультету кібербезпеки, програмної інженерії та комп'ютерних наук Міжнародного гуманітарного університету навчальна практика студентів денної та заочної форми навчання проводиться на 1 курсі протягом 4-х тижнів. Строки проведення навчальної 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 та «Положенням про практичну підготовку здобувачів вищої та фахової передвищої освіти Міжнародного гуманітарного університету», затвердженим Вченою радою Міжнародного гуманітарного університету 6 липня 2023 року (протокол №7).

Метою навчальної практики є закріплення теоретичних знань, які були одержані в процесі навчання, формування в студента професійного вміння приймати самостійні рішення

в певних виробничих умовах, оволодіння студентами сучасними технологіями, навичками та знаннями в галузі майбутньої спеціальності 125 Кібербезпека та захист інформації

Загальними завданнями практики є:

- ознайомитися з організацією освітнього процесу в закладі освіти та документацією;
- формування уявлень про основні вимоги до програмного забезпечення, що вирішує завдання захисту інформації;
- формування інтегральної компетентності, необхідної для розв'язання простих спеціалізованих задач у галузі кібербезпеки та захисту інформації.

Передумовами для навчальної практики є знання і вміння, отримані здобувачем з дисциплін, що вивчалися протягом першого семестру.

Зміст навчальної практики – ознайомлення студентів-практикантів зі структурою закладу освіти і загальною організацією місця проходження практики; навчання практичним прийомам обробки даних у комп'ютерних системах; ознайомлення з нормативною і технічною документацією комп'ютерних інформаційних систем, а також програмним, технічним, інформаційним і організаційним забезпеченням комп'ютерного кабінету або спеціалізованого комп'ютерного класу.

Завдання практики: закріплення і практичне використання теоретичних знань; розвиток особистісних професійних здібностей, виховання почуття поваги до професії; початкове накопичення професійного досвіду, поглиблення та вдосконалення знань, умінь, навичок; формування творчого, дослідницького підходу до професійної діяльності.

Знання і вміння, які отримує здобувач, залежать безпосередньо від бази практики, куди він направляється. Кожна із баз практики може надати перелік вимог щодо оволодіння тією чи іншою інформацією про базу практики, який дасть змогу здобувачеві чітко визначити подальший план ознайомлення його з базою практики.

Мова навчання – українська.

Статус навчальної дисципліни – обов'язкова навчальна дисципліна.

В результаті проходження навчальної практики здобувач набуває наступні компетентності, передбачені освітньою програмою «Кібербезпека та захист інформації».

Інтегральна компетентність

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово

ЗК 4. Здатність спілкуватися іноземною мовою

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями

ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

ЗК 7. Здатність ухвалювати рішення и діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

ЗК 8. 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 форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні) компетентності (СК)

СК 1. Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації

Результати навчання

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

РН 3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброочесності у професійній діяльності.

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність

РН 5. 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

РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН 7. Застосовувати й 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

РН 8. Застосовувати знання и розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

2.4.2 Технологічна практика

Технологічна 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 першого (бакалаврського) рівня вищої освіти. Технологічна практика проводиться на другому курсі протягом 4 тижнів і має обсяг 6 кредитів ЄКТС (180 годин). Технологічна практика проводиться з метою поглиблення та систематизації професійних знань, отриманих у процесі навчання, а також формування в студентів цілісного розуміння технологічних процесів, що лежать в основі забезпечення кібербезпеки; вона сприяє розвитку практичних умінь з проектування, реалізації та супроводу безпечних інформаційних систем, ознайомлює з реальними виробничими умовами, вимогами до професійної діяльності фахівця з кібербезпеки. Технологічна практика проводиться в компаніях, що працюють у сферах освіти та інформаційних технологій, та активно використовують, впроваджують або створюють сучасні інтерактивні інструменти для навчання та навчально-методичні матеріали для забезпечення високоякісної освіти. Враховуючи специфіку роботи в сучасних компаніях, у яких активно використовується дистанційний формат роботи, практика може проходити як у очному – коли здобувач фізично присутній на території підприємства, так і дистанційному форматах.

Строки проведення технологічної 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 та «Положенням про практичну підготовку здобувачів вищої та фахової передвищої освіти Міжнародного гуманітарного університету», затвердженим Вченою радою Міжнародного гуманітарного університету 6 липня 2023 року (протокол №7).

Метою технологічної практики є формування цілісного практичного досвіду щодо застосування сучасних технологій, методів і засобів забезпечення кібербезпеки в реальних або модельованих умовах, поглиблення професійних компетентностей у галузі захисту інформаційних систем, розвиток здатності самостійно вирішувати типові завдання з проектування, адміністрування та моніторингу безпечних ІТ-середовищ, а також підготовка до виконання подальших навчальних, науково-дослідних та професійних завдань у відповідності до вимог освітньо-професійної програми.

Передумовами для технологічної практики є знання і вміння, отримані здобувачем під час бакалаврської підготовки.

Зміст технологічної практики – передбачає виконання комплексу практичних завдань, спрямованих на освоєння сучасних технологій забезпечення кібербезпеки, а також використання професійного програмного забезпечення для моніторингу, виявлення та реагування на кіберзагрози в умовах, що наближені до реальних.

Завдання практики: полягають у поглибленні та розширенні практичних навичок у проектуванні безпечних інформаційно-комунікаційних систем, реалізації заходів щодо запобігання, виявлення та реагування на кібератаки, застосування сучасних методів аналізу вразливостей та управління інцидентами безпеки, а також формування здатності до

самостійного прийняття технічних рішень у відповідності до професійних стандартів, чинного законодавства та вимог замовників або організацій.

Мова навчання – українська.

Статус навчальної дисципліни – обов'язкова навчальна дисципліна.

В результаті проходження технологічної практики здобувач набуває наступні компетентності, передбачені освітньою програмою «Кібербезпека та захист інформації».

Інтегральна компетентність

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово

ЗК 4. Здатність спілкуватися іноземною мовою

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями

ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

ЗК 7. Здатність ухвалювати рішення и діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

ЗК 8. 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 форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні) компетентності (СК)

СК 1. Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації

СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

Результати навчання

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

РН 3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність

РН 5. 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

РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН 7. Застосовувати й 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

РН 8. Застосовувати знання и розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації

РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

РН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

РН 17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

2.4.3 Виробнича практика

Виробнича 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 першого (бакалаврського) рівня вищої освіти. Виробнича практика проводиться на третьому курсі протягом 4 тижнів і має обсяг 6 кредитів ЄКТС (180 годин). Виробнича практика проводиться з метою формування у здобувачів уявлення про методологію наукової творчості, досвіду організації творчої діяльності, використання методів наукового пізнання та застосування логічних законів і правил, практичних навичок і умінь щодо праці у сфері освіти в умовах широкого застосування інформаційних технологій, обчислювальної техніки та методів системного аналізу у всіх галузях. Виробнича практика проводиться в компаніях, що працюють у сферах освіти та інформаційних технологій, та активно використовують, впроваджують або створюють сучасні інтерактивні інструменти для навчання та навчально-методичні матеріали для забезпечення високоякісної освіти. Враховуючи специфіку роботи в сучасних компаніях, у яких активно використовується дистанційний формат роботи, практика може проходити як у очному – коли здобувач фізично присутній на території підприємства, так і дистанційному форматах.

Строки проведення виробничої 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 та «Положенням про практичну підготовку здобувачів вищої та фахової передвищої освіти Міжнародного гуманітарного університету», затвердженим Вченою радою Міжнародного гуманітарного університету 6 липня 2023 року (протокол №7).

Метою виробничої практики є закріплення, поглиблення та розширення теоретичних знань, отриманих під час вивчення профільних дисциплін, а також формування практичних навичок і компетентностей, необхідних для виконання технологічних операцій у сфері кібербезпеки, зокрема в галузі захисту інформації, адміністрування безпечних систем та застосування сучасних методів і засобів забезпечення інформаційної безпеки.

Передумовами для виробничої практики є знання і вміння, отримані здобувачем під час бакалаврської підготовки.

Зміст виробничої практики – передбачає виконання комплексу практичних завдань, спрямованих на освоєння сучасних технологій забезпечення кібербезпеки, а також використання професійного програмного забезпечення для моніторингу, виявлення та реагування на кіберзагрози в умовах, що наближені до реальних.

Завдання практики: полягають у формуванні в студентів практичних навичок і професійних компетентностей, необхідних для реалізації технологічних процесів у сфері кібербезпеки, зокрема в оволодінні методами аналізу та оцінювання рівня захищеності інформаційних систем, застосуванні сучасних засобів захисту даних, налаштуванні безпечних мережевих середовищ, виявленні та усуненні вразливостей, а також у розумінні ролі технологічних рішень у забезпеченні цілісності, конфіденційності та доступності інформації відповідно до чинного законодавства та професійних стандартів.

Мова навчання – українська.

Статус навчальної дисципліни – обов'язкова навчальна дисципліна.

В результаті проходження виробничої практики здобувач набуває наступні компетентності, передбачені освітньою програмою «Кібербезпека та захист інформації».

Інтегральна компетентність

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово

ЗК 4. Здатність спілкуватися іноземною мовою

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями

ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

ЗК 7. Здатність ухвалювати рішення и діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

ЗК 8. 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 форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні) компетентності (СК)

СК 1. Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації

СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).

СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

СК 11. Здатність здійснювати проектування, адміністрування та керування інформаційно-комунікаційними системами, забезпечуючи їхню надійність, безпеку та ефективність функціонування.

Результати навчання

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

РН 3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність

РН 5. 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

РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН 7. Застосовувати й 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

РН 8. 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.

РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації

РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

РН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

РН 17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

РН 20. 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 і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

2.4.4 Переддипломна практика

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 першого (бакалаврського) рівня вищої освіти. Переддипломна практика проводиться на четвертому курсі у другому семестрі протягом 4 тижнів і має обсяг 6 кредитів ЄКТС (180 годин). Переддипломна практика проводиться з метою остаточного формування у здобувачів компетентностей, передбачених освітньо-професійною програмою, зокрема методології наукової творчості, досвіду організації творчої діяльності, використання методів наукового пізнання та застосування логічних законів і правил, практичних навичок і умінь щодо праці у сфері освіти в умовах широкого застосування інформаційних технологій, обчислювальної техніки та методів системного аналізу у всіх галузях. Переддипломна практика проводиться в компаніях, що працюють у сферах освіти та інформаційних технологій, та активно використовують, впроваджують або створюють сучасні інтерактивні інструменти для навчання та навчально-методичні матеріали

для забезпечення високоякісної освіти. Враховуючи специфіку роботи в сучасних компаніях, у яких активно використовується дистанційний формат роботи, практика може проходити як у очному – коли здобувач фізично присутній на території підприємства, так і дистанційному форматах.

Строки проведення переддипломної 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 та «Положенням про практичну підготовку здобувачів вищої та фахової передвищої освіти Міжнародного гуманітарного університету», затвердженим Вченою радою Міжнародного гуманітарного університету 6 липня 2023 року (протокол №7).

Метою переддипломної практики є закріплення здобувачами досвіду самостійної науково-дослідної роботи та застосування методики її проведення, результатом чого має стати збирання фактичного матеріалу для виконання кваліфікаційної роботи.

Головним завданням переддипломної практики є збір матеріалів для виконання випускної кваліфікаційної роботи. Матеріали, зібрані під час перебування на практиці, мають бути вихідними даними для розробки випускної кваліфікаційної роботи. Необхідні матеріали студент 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.

Мова навчання – українська.

Статус навчальної дисципліни – обов'язкова навчальна дисципліна.

В результаті проходження переддипломної практики здобувач набуває наступні компетентності, передбачені освітньою програмою «Кібербезпека та захист інформації».

Інтегральна компетентність

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово

ЗК 4. Здатність спілкуватися іноземною мовою

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями

ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

ЗК 7. Здатність ухвалювати рішення і діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

ЗК 8. 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 форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні) компетентності (СК)

СК 1. Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації

СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).

СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

СК 11. Здатність здійснювати проєктування, адміністрування та керування інформаційно-комунікаційними системами, забезпечуючи їхню надійність, безпеку та ефективність функціонування.

Результати навчання

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

РН 3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність

РН 5. 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

РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН 7. Застосовувати й 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

РН 8. Застосовувати знання и розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації

РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

РН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

РН 15. Збирати, обробляти зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводили аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

РН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

РН 17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

РН 20. 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 і контроль стану апаратних засобів захисту інформації та комплексів технічною захисту інформації.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

РН 22. Вміти застосовувати методи та інструменти проєктування й адміністрування мереж і систем, виконувати налаштування, моніторинг та підтримку їхньої працездатності з урахуванням вимог інформаційної безпеки.

3 ОРГАНІЗАЦІЯ ТА ПРОВЕДЕННЯ ПРАКТИКИ

3.1 Загальна організація практики

У процесі проведення практики приймають участь:

- здобувач першого (бакалаврського) рівня вищої освіти (далі – здобувач);
- керівник практики від кафедри інформаційних технологій (далі – керівник практики від кафедри);
- керівник практики від бази практики;
- навчальний відділ Міжнародного гуманітарного університету, декан факультету кібербезпеки, програмної інженерії та комп'ютерних наук, завідувач кафедрою комп'ютерної інженерії та інноваційних технологій та інші особи, які мають повноваження для перевірки проходження практики здобувачів першого (бакалаврського) рівня вищої освіти.

Загальну організацію практики здобувачів та контроль за її проведенням здійснює навчальний відділ Міжнародного гуманітарного університету.

Відповідальність за організацію, проведення і контроль проходження практики здобувачами покладається на декана факультету кібербезпеки програмної інженерії та комп'ютерних наук.

Безпосереднє навчально-методичне керівництво і виконання робочої програми практики забезпечує кафедра інформаційних технологій.

Звітною документацією здобувача про проходження практики є:

- щоденник практики;
- звіт з проходження практики.

Щоденник практики надається здобувачеві у паперовому або електронному вигляді керівником практики від кафедри перед початком практики. У щоденнику практики вказується індивідуальна інформація про здобувача (ПІБ, факультет, спеціальність, курс, назва освітньої програми, тощо), вид практики, назва бази практики, дати прибуття на базу практики та вибуття з неї (завірені покрою печаткою підприємства), календарний графік проходження практики, робочі записи здобувача, відгук та оцінка роботи здобувача (завірені покрою печаткою підприємства), відгуки та оцінки осіб, що керували та перевіряли проходження практики.

Звіт з проходження практики здобувач формує самостійно за результатами проходження практики, відповідно до вимог, визначених у робочій програмі практики. За необхідністю, звіт з проходження практики може бути попередньо перевірений керівником від бази практики на предмет наявності у ньому інформації, що містить державну або комерційну таємницю.

3.2 Вимоги до баз практики

Практика здобувачів вищої освіти 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 України та за її межами, які мають належні умови для проведення практики та відповідають профілю освітньої програми.

Визначення баз практики здійснюється кафедрою комп'ютерних наук 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'ютерних наук 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.

Перелік рекомендованих баз практик для здобувачів першого (бакалаврського) рівня факультету кібербезпеки, програмної інженерії та комп'ютерних наук, що навчаються за спеціальністю 125 – «Кібербезпека та захист інформації», і з якими Міжнародним гуманітарним університетом укладено договори про створення баз практики, наведено у таблиці 1.

Таблиця 1 – Перелік рекомендованих баз практик для здобувачів першого (бакалаврського) рівня 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	Управління протидії кіберзлочинам в Одеській області Департаменту кіберполіції Національної поліції України	Договір №044 від 18.11.2022
2	Освітній фонд «Кіпсолід»	Договір №040 від 16.11.2022
3	Приватне підприємство "Науково-виробниче підприємство "КАРЕ"	Договір №130/1 від 23.10.2024
4	ТОВ "Мітрідат Одеса"	Договір №125/1 від 18.01.2024
5	ТОВ "Юнейшн"	Договір №129/1 від 22.10.2024
6	ТОВ «Альфа ТВ»	Договір №042 від 02.11.2022
7	ТОВ «Гігабайт+»	Договір №043 від 10.11.2022
8	ТОВ «ЕЛАН-ІНЕТ»	Договір №041 від 07.11.2022
9	ТОВ «РЕНОМЕ СЕРВІС»	Договір №039 від 01.11.2022

Основні вимоги до підприємств, установ і організацій, державних органів та органів місцевого самоврядування, самозайнятих осіб, що можуть бути базами практики здобувачів фахової передвищої освіти:

- наявність структурних складових, що відповідають спеціальності 125 – «Кібербезпека та захист інформації»;
- наявність кваліфікованого персоналу, який може забезпечити належне керівництво практикою здобувачів першого (бакалаврського) рівня вищої освіти;
- можливість створення умов для проходження практики здобувачами;
- обов'язкове забезпечення безпечних умов проходження практики;
- можливість забезпечення необхідною робочою документацією, що відображає діяльність різних підрозділів бази практики;
- можливість користування бібліотекою, лабораторіями, технічною та іншою документацією, необхідною для виконання програми практики;
- наявність сучасного спеціалізованого інформаційного та технологічного забезпечення.

3.3 Обов'язки керівника практики від кафедри

Керівник практики від кафедри:

- розробляє робочу програму практики;
- погоджує робочу програму практики з гарантом освітньої програми, завідувачем кафедрою та начальником навчального відділу;
- розробляє (за необхідністю) індивідуальні завдання відповідно до розподілу здобувачів за місцями проходження практики;
- перевіряє наявність у здобувачів перед від'їздом на базу практики необхідних для проходження практики документів: направлення на базу практики, індивідуального завдання (за необхідністю), щоденника практики та інших документів;
- здійснює контроль за своєчасним прибуттям здобувачів до місць практики, виконанням програми практики та дотриманням термінів її проведення;
- повідомляє здобувачів про систему звітності з практики та порядок складання заліку практики за результатами проходження практики;
- разом з керівником від бази практики забезпечує високу якість її проходження згідно з робочою програмою практики;
- надає методичну допомогу під час виконання ними індивідуальних завдань і збору матеріалів для звітної документації;
- приймає залік практики здобувачів фахової передвищої освіти за результатами проходження практики;
- узагальнює результати проходження практики та формує письмовий звіт про проведення практики із зауваженнями і пропозиціями щодо її удосконалення.

3.4 Обов'язки керівника практики від бази практики

Керівник практики від бази практики:

- несе особисту відповідальність за проведення практики;
- організовує проходження практики згідно з робочою програмою практики та індивідуального завдання (за наявності);

- визначає робочі місця практики здобувачів;
- забезпечує ефективність проходження практики;
- забезпечує проведення інструктажу та дотримання здобувачами правил техніки безпеки й охорони праці на робочому місці;
- забезпечує виконання, погоджених з навчальним планом, графіків проходження практики у структурних підрозділах бази практики;
- сприяє використанню здобувачами наявної літератури, необхідної документації тощо;
- контролює дотримання здобувачами правил внутрішнього розпорядку;
- створює необхідні умови для оволодіння здобувачами новою технікою, сучасними технологіями та методами організації праці;
- складає у щоденнику практики відгук за результатом проходження практики;
- затверджує щоденник практики;
- виставляє оцінку роботи здобувачу за результатами проходження практики.

3.5 Обов'язки здобувача першого (бакалаврського) рівня вищої освіти

Здобувач першого (бакалаврського) рівня вищої освіти при проходженні практики зобов'язаний:

- до установчої конференції ознайомитися з «Положенням про практичну підготовку здобувачів вищої та фахової передвищої освіти Міжнародного гуманітарного університету», робочою програмою практики, а також формами документів звітної документації;
- до початку практики одержати на установчій конференції з практики направлення на практику та індивідуальне завдання (за необхідністю);
- перед початком практики пройти на кафедрі інструктаж з техніки безпеки;
- своєчасно прибути на базу практики;
- у повному обсязі виконувати всі завдання, передбачені робочою програмою практики і вказівки керівників практики;
- вивчити і суворо дотримуватись правил охорони праці, техніки безпеки і виробничої санітарії;
- нести відповідальність за виконані завдання;
- щодня в хронологічному порядку детально відображати у розділі «Робочі записи» щоденника практики характер навчально-практичної активності з коротким аналізом і висновками, у тому числі щодо досягнення результатів навчання;
- подати керівникам практики звітні документи, скласти залік з практики.

Здобувач має право на безоплатне проходження практики на підприємствах, в установах, закладах та організаціях.

Здобувач має право надавати пропозиції щодо поліпшення практики, покращення її загальних результатів, вказувати на проблемні моменти під час проходження практики.

4 КАЛЕНДАРНО-ТЕМАТИЧНІ ПЛАНИ ПРАКТИКИ

У цьому розділі наведені календарно-тематичні плани проходження практики. Вони є орієнтовним і можуть змінюватися, залежно від бази практики та індивідуального завдання здобувача (за наявності). Індивідуальні календарно-тематичні плани здобувачів та усі зміни до них повинні бути попередньо узгодженими із керівниками від кафедри та бази практики.

4.1 Календарний план навчальної практики

Тиждень 1

	Тема	Кі лькість годин
	Знайомство із керівниками практики від університету та бази практики, темою та завданням практики, правилами оформлення звітної документації	6
	Знайомство із базою практики (історія створення, напрями діяльності, види товарів, що виробляються, чи послуг, що надаються)	2

	Інструктаж із техніки безпеки та охорони праці на базі практики в цілому	2
	Організаційні заходи (розподіл по робочим місцям, прибуття на робочі місця, знайомство із безпосереднім керівником практики)	4
	Ознайомлення з проєктом (призначення, особливості тощо)	4
	Інструктаж з техніки безпеки та охорони праці на робочому місці	2
	Ознайомлення із посадовими інструкціями на робочому місці та завданнями, які будуть виконуватись протягом практики	16
	Підготовка матеріалів для звіту з практики	9
	Загалом	45

Тиждень 2, 3

	Тема	Кі лькість годин
	Організаційні заходи (розподіл завдань, участь у виробничих нарадах тощо)	10
	Виконання завдань безпосереднього керівника практики (залежно від бази практики: монтаж, налаштування чи обслуговування комп'ютерного обладнання, монтаж, налаштування чи адміністрування інформаційних мереж, розробка чи налаштування програмного забезпечення, робота з контрольно-вимірювальними приладами, розробка чи адміністрування вебсайтів, розробка чи адміністрування баз даних, розробка чи відновлення вузлів комп'ютерної техніки тощо)	60
	Підготовка матеріалів для звіту з практики	20
	Загалом	90

Тиждень 4

	Тема	Кі лькість годин
	Консультації із керівниками практики від університету та бази практики стосовно підготовки звітних документів	15
	Підготовка звітних документів (щоденник, звіт з практики)	30
	Загалом	45

4.2 Календарний план технологічної практики

Тиждень 1

	Тема	Кількість годин
	Знайомство із керівниками практики від університету та бази практики, темою та завданням практики, правилами оформлення звітної документації	6
	Знайомство із базою практики (історія створення, напрями діяльності, види товарів, що виробляються, чи послуг, що надаються)	2

	Інструктаж із техніки безпеки та охорони праці на базі практики в цілому	2
	Організаційні заходи (розподіл по робочим місцям, прибуття на робочі місця, знайомство із безпосереднім керівником практики)	4
	Ознайомлення з проєктом (призначення, особливості тощо)	4
	Інструктаж з техніки безпеки та охорони праці на робочому місці	2
	Ознайомлення із посадовими інструкціями на робочому місці та завданнями, які будуть виконуватись протягом практики	16
	Підготовка матеріалів для звіту з практики	9
	Загалом	45

Тиждень 2, 3

	Тема	Кількість годин
	Організаційні заходи (розподіл завдань, участь у виробничих нарадах тощо)	10
	Виконання завдань безпосереднього керівника практики (залежно від бази практики: монтаж, налаштування чи обслуговування комп'ютерного обладнання, монтаж, налаштування чи адміністрування інформаційних мереж, розробка чи налаштування програмного забезпечення, робота з контрольно-вимірювальними приладами, розробка чи адміністрування вебсайтів, розробка чи адміністрування баз даних, розробка чи відновлення вузлів комп'ютерної техніки тощо)	60
	Підготовка матеріалів для звіту з практики	20
	Загалом	90

Тиждень 4

	Тема	Кількість годин
	Консультації із керівниками практики від університету та бази практики стосовно підготовки звітних документів	15
	Підготовка звітних документів (щоденник, звіт з практики)	30

	Загалом	45
--	---------	----

4.3 Календарний план виробничої практики

Тиждень 1

№	Тема	Кількість годин
1	Знайомство із керівниками практики від кафедри та бази практики, темою та завданням практики, правилами оформлення звітної документації	6
2	Знайомство із базою практики (історія створення, напрями діяльності, види товарів, що виробляються, чи послуг, що надаються)	2
3	Інструктаж із техніки безпеки та охорони праці на базі практики в цілому	2
4	Організаційні заходи (розподіл по робочим місцям, прибуття на робочі місця, знайомство із безпосереднім керівником практики)	4
5	Ознайомлення з проєктом (призначення, особливості тощо), в якому здобувач буде приймати безпосередню участь	4
6	Інструктаж з техніки безпеки та охорони праці на робочому місці	2
7	Ознайомлення із посадовими інструкціями на робочому місці та завданнями, які будуть виконуватись протягом практики	16
8	Підготовка матеріалів для звіту з практики	9
	Загалом	45

Тиждень 2, 3

№	Тема	Кількість годин
1	Організаційні заходи (розподіл завдань, участь у виробничих нарадах тощо)	10
2	Виконання завдань безпосереднього керівника практики (залежно від бази практики: підготовка та/або проведення освітніх заходів (лекцій, практик, лабораторних занять, семінарів, конференцій, круглих столів, хакатонів тощо), навчально-методичної літератури, технічних та програмних засобів для проведення освітніх заходів тощо)	60
3	Підготовка матеріалів для звіту з практики	20
	Загалом	90

Тиждень 4

№	Тема	Кількість годин
1	Консультації із керівниками практики від кафедри та бази практики стосовно підготовки звітних документів	15
2	Підготовка звітних документів (щоденник, звіт з практики)	30
	Загалом	45

4.4 Календарний план переддипломної практики

Тиждень 1

№	Тема	Кількість годин
1	Знайомство із керівниками практики від кафедри та бази практики, темою та завданням практики, правилами оформлення звітної документації	6
2	Знайомство із базою практики (історія створення, напрями діяльності, види товарів, що виробляються, чи послуг, що надаються)	2

3	Інструктаж із техніки безпеки та охорони праці на базі практики в цілому	2
4	Обговорення змісту переддипломної практики та обсягом досліджень, запланованих в кваліфікаційній роботі, знайомство із безпосереднім керівником практики	4
5	Ознайомлення із робочим місцем (обладнання, програмне забезпечення, техніка безпеки, посадові інструкції тощо)	4
6	Інструктаж з техніки безпеки та охорони праці на робочому місці	2
7	Підготовка до проведення досліджень, запланованих у кваліфікаційній роботі	16
8	Підготовка матеріалів для звіту з практики	9
	Загалом	45

Тиждень 2, 3

№	Тема	Кількість годин
1	Організаційні заходи (розподіл завдань, участь у виробничих нарадах тощо)	10
2	Проведення досліджень, запланованих у кваліфікаційній роботі, залежно від теми кваліфікаційної роботи: підготовка та/або проведення освітніх заходів (лекцій, практик, лабораторних занять, семінарів, конференцій, круглих столів, хакатонів тощо), навчально-методичної літератури, технічних та програмних засобів для проведення освітніх заходів тощо.	60
3	Підготовка матеріалів для звіту з практики	20
	Загалом	90

Тиждень 4

№	Тема	Кількість годин
1	Консультації із керівниками практики від кафедри та бази практики стосовно підготовки звітних документів	15
2	Підготовка звітних документів (щоденник, звіт з практики)	30
	Загалом	45

5 ОФОРМЛЕННЯ РЕЗУЛЬТАТІВ ПРОВЕДЕННЯ ПРАКТИКИ

Після закінчення практики здобувачі звітують про виконання програми практики шляхом оформлення звіту з використанням матеріалів, з якими вони безпосередньо працювали на базі практики. Звіт повинен мати чітко структуровану послідовність, переконливу аргументацію, обґрунтованість рекомендацій та висновки.

Оформлення звіту повинно відповідати вимогам ДСТУ 3008:2015 «Звіти у сфері науки і техніки. Структура та правила оформлення».

Звіт складається з:

- титульної сторінки;
- змісту, який містить назви всіх розділів із зазначенням сторінок, на яких вони викладені;
- мети та змісту проходження практики;
- основної частини;
- висновків;
- списку використаних джерел;
- додатків (за необхідності).

Основна частина звіту поділяється на розділи, перелік і послідовність яких визначаються змістом програми практики. Загальний обсяг звіту – не більше 20 сторінок формату А4, надрукованих або охайно написаних від руки.

У звіті здобувач висвітлює, крім питань програми практики, спірні питання, що виникли в процесі проходження практики, особисті зауваження, враження і пропозиції щодо удосконалення діяльності бази практики.

Відгук керівника від бази практики може бути виконаний на окремому аркуші, або розташовуватись у відповідному розділі щоденника практики. Відгук керівника від бази практики засвідчується керівником бази практики 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 оцінку його діяльності за «п'ятибальною» шкалою.

Письмовий звіт разом із заповненим щоденником практики та відгуком керівника від бази практики подається на рецензування керівникові практики від кафедри, який має відобразити рівень засвоєних здобувачем теоретичних знань та умінь застосовувати їх на практиці, відомості про виконання здобувачем усіх розділів програми практики, правильності оформлення звітної документації, висновки і пропозиції щодо оцінки практики при її захисті.

Здобувач захищає звіт про проходження практики після своєчасного подання матеріалів навчальної практики у призначений керівником від кафедри день.

Захист практики може приймати комісія, до складу якої входять викладачі, які проводять заняття, представники адміністрації Міжнародного гуманітарного університету, представники баз практики. За результатами захисту виставляється диференційована оцінка, яка фіксується на титульному аркуші звіту, у відомості та заліковій книжці.

У разі невиконання програми практики або неподання звітних матеріалів керівникові практики від кафедри здобувачеві виставляється незадовільна оцінка і він направляється на повторне проходження практики.

6 КРИТЕРІЇ ОЦІНКИ ЗНАНЬ ЗДОБУВАЧІВ

До критеріїв оцінювання результатів проходження практики, а також перевірки рівня сформованості умінь та навичок здобувачами передвищої освіти відносяться:

- своєчасне проведення робіт, що зазначені у завданні на практику, індивідуальному завданні (за наявності) та календарно-тематичному плані практики;
- своєчасне надання керівникові від кафедри матеріалів практики згідно завдання на практику або індивідуального завдання (за наявності);
- якісна підготовка здобувачем звіту з проходження практики;
- підготовка здобувача до захисту звіту з проходження практики та індивідуального завдання (за наявності).

Успішність оцінювання здійснюється за такими критеріями:

- відповідність змісту звіту з проходження практики темі завдання;
- наявність глибоко продуманої в усіх її частинах програми дослідження;
- успішність виконання завдання;
- літературне, технічне та естетичне оформлення звіту;
- вчасне подання звіту керівникові практики від кафедри на перевірку та оцінювання.

Проходження практики оцінюється на:

– **«Зараховано» («Відмінно», «А», 90 – 100 балів)** – якщо здобувач має щоденник з практики, завірений мокрими печатками підприємства бази практики, був присутній на базі практики не менше ніж 90% часу, а у звіті з проходження практики наведено не менше ніж 90% інформації про розв’язання поставленого завдання. При цьому звіт з практики повністю розкриває поставлене завдання, містить теоретичний матеріал, який органічно сполучений з практичним, а його оформлення повністю відповідає вимогам до оформлення звіту з практики.

– **«Зараховано» («Добре», «В», 82 – 89 балів)** – якщо здобувач має щоденник з практики, завірений мокрими печатками підприємства бази практики, був присутній на базі практики не менше ніж 80% часу, а у звіті з проходження практики наведено не менше ніж 80% інформації про розв’язання поставленого завдання. При цьому звіт з практики не повністю розкриває поставлене завдання, не містить теоретичного матеріалу а його оформлення має незначні відхилення від вимог до оформлення звіту з практики.

– **«Зараховано» («Добре», «С», 74 – 81 балів)** – якщо здобувач має щоденник з практики, завірений мокрими печатками підприємства бази практики, був присутній на базі практики не менше ніж 75% часу, а у звіті з проходження практики наведено не менше ніж 75% інформації про розв’язання поставленого завдання. При цьому звіт з практики не повністю розкриває поставлене завдання, не містить теоретичного матеріалу, а його оформлення має систематичні відхилення від вимог до оформлення звіту з практики.

– **«Зараховано» («Задовільно», «D», 64 – 73 балів)** – якщо здобувач має щоденник з практики, завірений мокрими печатками підприємства бази практики, був присутній на базі практики не менше ніж 70% часу, а у звіті з проходження практики наведено не менше ніж 70% інформації про розв’язання поставленого завдання. При цьому звіт з практики містить фрагментовану інформацію про поставлене завдання, істотну кількість запозичень із відкритих джерел, а його оформлення має систематичні відхилення від вимог до оформлення звіту з практики.

– **«Зараховано» («Задовільно», «E», 60 – 63 балів)** – якщо здобувач має щоденник з практики, завірений мокрими печатками підприємства бази практики, був присутній на базі практики не менше ніж 60% часу, а у звіті з проходження практики наведено не менше ніж 60% інформації про розв’язання поставленого завдання. При цьому звіт з практики містить фрагментовану інформацію про поставлене завдання, істотну кількість запозичень із відкритих джерел, а його оформлення значно відрізняється від вимог до оформлення звіту з практики.

– **«Не зараховано» («Незадовільно з можливістю повторного складання», «FX», 35 – 59 балів)** – якщо здобувач має щоденник з практики, завірений мокрими печатками підприємства бази практики, був присутній на базі практики не менше ніж 60% часу, але у звіті з проходження практики наведено менше 60% інформації про розв’язання поставленого завдання. При цьому звіт з практики містить фрагментовану інформацію, запозичену із відкритих джерел, які не стосуються суті завдання з практики, а його оформлення значно відрізняється від вимог до оформлення звіту з практики.

– **«Не зараховано» («незадовільно з обов’язковим повторним проходженням практики», «F», 1 – 34 балів)** – якщо здобувач не має щоденника з практики, завіреного мокрими печатками підприємства бази практики, або був присутній на базі практики менше ніж 60% часу.

Таблиця відповідності результатів контролю знань за різними шкалами

100-бальна шкала	Шкала за ECTS	Національна шкала	
		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		

7 РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. 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.
2. 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.
3. ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання - Введ.01.07.2016. - Київ: Держстандарт України, 2016. – 20 с.
4. Положення про практичну підготовку здобувачів вищої та фахової передвищої освіти Міжнародного гуманітарного університету» (затверджено Вченою радою Міжнародного гуманітарного університету 6 липня 2023 року, протокол №7), МГУ, 2023.
5. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник Київ: ООО Д.В.К., 2004. - 508 с
6. Замула О.А., Горбенко Ю.І., Шумов А.І. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації»: Навч. посібник. - Харків: ХНУРЕ, 2010
7. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва онографія. – К. : НІСД, 2014. – 328 с.
8. Курко А. М. Введення в теорію інформації //Посібник до вивчення дисципліни «Теорія інформації» / А. М. Курко, В. Я. Решетняк. Тернопіль: Тернопільський національний технічний університет ім. І. Пулюя. 2017 – 108с.
9. Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security // International Technical Support Organization. – Dec. 2010.
10. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В.Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний, Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178 с
11. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

Допоміжна

12. 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.

13. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту 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 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

Інформаційні ресурси

16. Національна бібліотека України ім. В.І. Вернадського. URL: <http://www.nbuv.gov.ua>.
17. Он-лайн бібліотека. URL: <http://www.lib.com.ua>.

3	Інструктаж із техніки безпеки та охорони праці на базі практики в цілому	2
4	Обговорення змісту переддипломної практики та обсягом досліджень, запланованих в кваліфікаційній роботі, знайомство із безпосереднім керівником практики	4
5	Ознайомлення із робочим місцем (обладнання, програмне забезпечення, техніка безпеки, посадові інструкції тощо)	4
6	Інструктаж з техніки безпеки та охорони праці на робочому місці	2
7	Підготовка до проведення досліджень, запланованих у кваліфікаційній роботі	16
8	Підготовка матеріалів для звіту з практики	9
	Загалом	45

Тиждень 2, 3

№	Тема	Кількість годин
1	Організаційні заходи (розподіл завдань, участь у виробничих нарадах тощо)	10
2	Проведення досліджень, запланованих у кваліфікаційній роботі, залежно від теми кваліфікаційної роботи: підготовка та/або проведення освітніх заходів (лекцій, практик, лабораторних занять, семінарів, конференцій, круглих столів, хакатонів тощо), навчально-методичної літератури, технічних та програмних засобів для проведення освітніх заходів тощо.	60
3	Підготовка матеріалів для звіту з практики	20
	Загалом	90

Тиждень 4

№	Тема	Кількість годин
1	Консультації із керівниками практики від кафедри та бази практики стосовно підготовки звітних документів	15
2	Підготовка звітних документів (щоденник, звіт з практики)	30
	Загалом	45

5 ОФОРМЛЕННЯ РЕЗУЛЬТАТІВ ПРОВЕДЕННЯ ПРАКТИКИ

Після закінчення практики здобувачі звітують про виконання програми практики шляхом оформлення звіту з використанням матеріалів, з якими вони безпосередньо працювали на базі практики. Звіт повинен мати чітко структуровану послідовність, переконливу аргументацію, обґрунтованість рекомендацій та висновки.

Оформлення звіту повинно відповідати вимогам ДСТУ 3008:2015 «Звіти у сфері науки і техніки. Структура та правила оформлення».

Звіт складається з:

- титульної сторінки;
- змісту, який містить назви всіх розділів із зазначенням сторінок, на яких вони викладені;
- мети та змісту проходження практики;
- основної частини;
- висновків;
- списку використаних джерел;
- додатків (за необхідності).