****

**УКРАЇНА**

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

**«КИЇВСЬКИЙ ПОЛІТЕХНИЧНИЙ ІНСТИТУТ**

**імені ІГОРЯ СІКОРСЬКОГО»**

03056, м. Київ, пр.-т Перемоги, 37

Навчально-науковий фізико-технічний інститут

«Затверджено»

Директор ННФТІ

\_\_\_\_\_\_\_\_\_\_\_\_ Олексій НОВІКОВ

«13» квітня 2023р.

М.П.

**У З Г О Д Ж Е Н О :**

Головний спеціаліст підприємства: Завідувач кафедри:

Дмитро ЛАНДЕ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2023 р. «13» квітня 2023 р.

**РОБОЧА ПРОГРАМА**

проведення **переддипломної** практики здобувачів вищої освіти бакалаврського рівня 4 курсу

зі спеціальності **125 Кібербезпека**

на підприємстві \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

з 17.04.2023 р. по 21.05.2023р.

**1. Вступ:** практика - це практична частина навчального процесу, яка проводиться перед написанням і захистом дипломного проекту.

Практика дозволяє здобувачам вищої освіти скористатися теоретичними знаннями, навичками і вміннями, зібрати матеріали для написання і захисту дипломної роботи. У процесі проходження практики, майбутні випускники, підбирають всякого роду інформацію про підприємство, на якому вони проходять практику - звітність, баланси, техніко-економічні показники та інші дані. Після проходження практики здобувачі вищої освіти обов'язково складають у письмовому вигляді звіт про її проходження.

***Обов'язки керівників практики від кафедри***

Для безпосереднього наукового керівництва практикою кожного здобувача вищої освіти відповідно до навчального навантаження викладачів, кафедрою призначаються керівники практики, які, зазвичай, є керівниками дипломних робіт.

*Обов'язки безпосередніх керівників практики, призначених кафедрами:*

* здійснює контроль прибуття здобувачів вищої освіти на практику та подає відомості про їх прибуття директору Інституту;

– надає допомогу здобувачеві вищої освіти у виборі теми наукових досліджень;

– надає консультації щодо проведення здобувачем вищої освіти ретельного та всебічного вивчення літературних джерел;

– надає роз’яснення з принципових питань, які виникають у здобувача вищої освіти щодо організації процесу наукової творчості;

* здійснює, у разі необхідності, разом з керівником-організатором практики від кафедри, вибірковий контроль за проходженням практики здобувачами вищої освіти безпосередньо на базі практики.

***Обов’язки керівника практики від підприємства (організації)***

Керівник практики від підприємства – бази практики зобов’язаний:

– разом із керівником практики від кафедри розподілити здобувачів вищої освіти по підрозділах бази практики (у разі необхідності);

– здійснювати методичне керівництво і надавати допомогу здобувачам вищої освіти в одержанні необхідних матеріалів для виконання програми практики;

– контролювати роботу здобувачів вищої освіти, ведення ними щоденників практики і додержання трудової дисципліни;

– інформувати керівника практики від кафедри в разі порушення здобувачем вищої освіти трудової дисципліни;

– перевіряти звіти про практику.

Керівник практики від підприємства перевіряє складений та оформлений відповідно до вимог звіт про практику, засвідчує його підписом і печаткою. У щоденнику коротко характеризує діяльність здобувача вищої освіти за час проходження практики.

***Обов’язки здобувачів вищої освіти*** ***-практикантів***

Здобувачі вищої освіти Інституту при проходженні практики зобов’язані:

– до початку практики на настановчих зборах, а далі в індивідуальному порядку

одержати від керівника практики консультації щодо проходження практики і оформлення всіх необхідних документів;

– своєчасно (не пізніше зазначеної у направленні дати) прибути на базу практики;

* систематично працювати над виконанням завдань за програмою практики;

– вести щоденник практики, в якому фіксувати виконання відповідних етапів (розділів) календарного плану-графіку практики;

– у повному обсязі виконувати всі завдання, передбачені програмою практики, зазначені у індивідуальному графіку проходження практики, та вказівками безпосереднього керівника;

– виконувати діючі на підприємстві (в організації) правила внутрішнього розпорядку;

– нести відповідальність за виконану роботу;

– постійно підтримувати контакти з кафедрою та у призначений керівником практики від кафедри термін з’явитися на проміжний контроль;

– висвітлити результати виконаної роботи та оформити їх у звіті про проходження практики, відповідно до встановлених і діючих вимог Інституту до структури та оформлення звіту;

* своєчасно надати на кафедру звітні документи та у належний термін захистити матеріали практики перед відповідною комісією.

**2. Мета і завдання практики:**

Переддипломна практика є важливою складовою бакалаврської програми підготовки бакалавра з кібербезпеки і має на меті систематизацію, розширення і закріплення професійних знань, формування у бакалаврів початкової компетенції ведення самостійної наукової роботи, дослідження та експериментування.

Суть переддипломної практики полягає у залученні бакалаврів до самостійної дослідницької роботи, ознайомленні з методикою проведення науково-дослідної роботи в академічних та спеціалізованих інститутах, провідних компаніях.

Метою та завданнями практики є :

- оволодіння студентами сучасними методами, навичками, вміннями та способами організації праці майбутньої професійної діяльності;

- формування одержаних знань професійних навичок та вмінь для прийняття самостійних рішень під час роботи;

- виховання потреби систематично поповнювати свої знання і застосовувати їх в практичній діяльності;

- здобути навички роботи зі спеціальною літературою, патентними матеріалами. Навчитися оформляти документацію з програмного забезпечення.

- вміти підготувати наукову статтю, доповідь, реферат за матеріалами самостійних досліджень;

- проводити науково-дослідні, проектні та супроводжувальні роботи.

Здобувач вищої освіти повинен вміти:

- на основі набутих теоретичних і практичних знань уміти вирішити конкретну наукову проблему; розробити комплексні підходи до її вивчення;

- уміти провести експериментальні дослідження, обробити результати і довести їх правомірність;

- узагальнювати і систематизувати отримані результати.

Предметом переддипломної практики є поглиблення навичок самостійної дослідницької роботи, розширення наукового світогляду бакалаврів, дослідження проблем практики та вміння пов’язувати їх з обраним теоретичним напрямком дослідження, визначати структуру та логіку майбутньої бакалаврської роботи.

У процесі проходження переддипломної практики у відповідності до освітньо-наукової програми «Кібербезпека» підготовки бакалавра з кібербезпеки спеціальності 125 – Кібербезпека має оволодіти такими *загальними компетентностями*:

- ЗК1 Здатність застосовувати знання у практичних ситуаціях;

- ЗК 2 Знання та розуміння предметної області та розуміння професії;

- ЗК 3 Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово;

- ЗК4 Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;

- ЗК 5 Здатність до пошуку, оброблення та аналізу інформації;

- ЗК6 Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права*,* прав і свобод людини і громадянина в Україні;

- ЗК 7 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.

Щодо опанування *спеціальних (професійних, фахових) компетентностей***,** а саме:

- ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

- ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/ або кібербезпеки.

- ФК 3. Здатність до використання програмних та програмно- апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

- ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

- ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

- ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.

- ФК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно- правових, організаційних та технічних засобів і методів, процедур,практичних прийомів та ін.).

- ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

- ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

- ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

- ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/ або кібербезпеки.

- ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та*/*або кібербезпеки.

- ФК 13. Здатність розв’язувати задачі за фахом із використанням математичних методів, алгоритмів, прикладних та системних програмних рішень та технологій.

- ФК 14. Здатність розв’язувати задачі із забезпечення конфіденційності, цілісності, доступності та спостережності інформації та керування нею із використанням сучасних технологій, моделей та методів кібербезпеки із врахуванням вимог нормативних документів та Стандартів.

- ФК 15. Здатність до аудиту кібербезпеки інформаційних систем, та управління інформаційною та кібернетичною безпекою.

- ФК 16. Здатність до проектування та розробки захищених інформаційних систем.

- ФК 17. Здатність до зворотної розробки та аналізу програмного забезпечення.

Завданням дисципліни «Переддипломна практика» є набуття *програмних результатів навчання*, знань та умінь, що безпосередньо стосуються науково-дослідної діяльності, а саме:

- РН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

- РН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

- РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

- РН 4. Аналізувати, аргументувати приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

- РН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

- РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

- РН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та */*або кібербезпеки.

- РН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та */*або кібербезпеки.

- РН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та*/*або кібербезпеки.

- РН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

- РН 11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.

- РН 12. Розробляти моделі загроз та порушника.

- РН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

- РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

- РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

- РН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

- РН 17. Забезпечувати процеси захисту та функціонування інформаційно- телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

- РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

- РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

- РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

- РН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

- РН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

- РН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

- РН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

- РН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

- РН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

- РН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

- РН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

- РН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційних та інформаційно- телекомунікаційних системах, ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

- РН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

- РН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

- РН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

- РН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

- РН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

- РН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.

- РН 36. Виявляти небезпечні сигнали технічних засобів.

- РН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

- РН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

- РН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

- РН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

- РН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

- РН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

- РН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

- РН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

- РН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

- РН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

- РН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

- РН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах

- РН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

- РН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних,сигнатурних, статистично-сигнатурних).

- РН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

- РН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

- РН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

- РН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

- РН 55. Здійснювати зворотну розробку та аналіз шкідливого програмного забезпечення із застосуванням сучасних технологій та математичних методів.

- РН 56. Застосовувати сучасні методи та технології аналізу та моніторингу кібернетичної безпеки для забезпечення управління інформаційною безпекою.

- РН 57. Здійснювати управління інцидентами безпеки із застосуванням ризик-орієнтованого підходу.

- РН 58. Володіти принципами проектування та системної інженерії захищених систем.

- РН 59. Здійснювати технічний аудит кібербезпеки, аудит кіберінцидентів.

**3. Організація проведення практики**

Організація та проведення практики регламентовані наступними документами:

- наказ по університету про направлення на практику і призначення керівників;

- робоча програма (силабус) практики;

- щоденники, робочі програми та індивідуальні завдання для проходження практики;

- графіки відвідування керівниками практики занять з метою здійснення контролю;

- звіти про виконання програми практики;

- екзаменаційні відомості щодо заліку з практики.

Відповідальність за організацію, проведення і контроль практик покладається на завідувача відповідної кафедри.

Для керівництва практикою завідувачем кафедри призначаються керівники практики від університету (кафедри).

Керівник практики від кафедри повинен:

- провести збори з бакалаврами та ознайомити їх з робочими програмами практики;

- видати щоденники та робочі програми;

- контролювати проходження практики;

- систематично, не рідше одного разу в тиждень, консультувати магістрів та контролювати етапи виконання програми практики згідно календарного плану;

- брати участь у прийняті заліків з практики;

- подати до деканату звіт про результати проведення практики з пропозиціями щодо її удосконалення.

Підсумки практики обов’язково обговорюються на засіданнях кафедри і засіданнях Вченої ради факультету/інституту.

Переддипломна практика розпочинається з проведення настановної конференції, в якій беруть участь здобувачі, керівник практики від випускаючої кафедри.

Місце проходження практики бакалаврів – наукові лабораторії кафедри, інститути НАНУ, організації -партнери.

Здобувачів вищої освіти ознайомлюють із наказом ректора, програмою та завданнями практики, тривалістю робочого часу на практиці, правилами внутрішнього розпорядку та правилами техніки безпеки, про що здійснюються відповідні записи в листку обліку проведення інструктажу з техніки безпеки та формою звітності.

На першому етапі бакалаври знайомляться:

1) з нормативними документами, які регламентують організацію навчального процесу у ЗВО;

2) з методичними знаннями організації та ведення наукового дослідження за темою магістерської дисертації, а саме:

- вирішення комплексних наукових та інженерно-технічних завдань у галузі захисту інформації в ІКС;

- виявлення закономірностей, систематизація і поглиблення проблем, явищ, інноваційних рішень тощо;

- виявлення теоретичних, методологічних та організаційних проблем захисту інформації в ІКС;

- розробка конкретних науково-виробничих задач експериментального і прикладного характеру;

- набуття навиків захисту власних рішень.

На заключному етапі практики відбувається підсумкова конференція з обговоренням результатів проведених досліджень, підготовка бакалаврами звіту за результатами проходження практики, його захист та залік.

**4. Зміст практики**

На навчальну дисципліну «Переддипломна практика» відводиться 180 годин / 6 кредитів ECTS, семестрова атестація – залік.

Виходячи з цілей та завдань переддипломної практики, можна виділити наступні необхідні заходи з дослідження цілей і завдань практики, що поставлені на даному етапі навчання.

Здобувач вищої освіти повинен вміти написати невелику наукову доповідь на тему, пов΄язану з індивідуальним завданням, в чому проявиться його вміння професійно зробити огляд спеціальної наукової літератури та патентних матеріалів у заданому напрямку. У дослідній частині роботи необхідно показати вміння теоретично обгрунтувати вирішення проблеми. Після цього – привести алгоритми і методи розв΄язання поставленої задачі, а також програмну реалізацію.

В період переддипломної практики здобувач вищої освіти повинен ознайомитись з сучасною науковою тематикою провідних наукових установ, отримати навички роботи з науковими методами досліджень, інформаційними пакетами, прикладним програмним забезпеченням щодо теми його індивідуального завдання; взяти участь в розробленні програмного або прикладного забезпечення. Здобувач вищої освіти повинен навчитись порядку ведення документації, яка супроводжує наукові дослідження та програмне забезпечення.

Тривалість навчальної дисципліни «Переддипломна практика» – п’ять тижнів.

**5. Календарний план проведення практики:**

|  |  |  |
| --- | --- | --- |
| **№** | **Зміст** | **Термін виконання** |
| 1 | Прибуття студентом на практику, оформлення, отримання перепусток | 17.04.23 |
| 2 | Проведення інструктажу з техніки безпеки, охорони праці | 17.04.23 |
| 3 | Проведення екскурсій по підприємству, ознайомлення з місцем роботи |  |
| 4 | Виконання програми практики і індивідуального завдання | Впродовж всієї практики |
| 5 | Оформлення щоденника, звіту, складання заліку з практики | 15.05 – 21.05.23 |

**6. Вимоги до звіту**

Звіт з практики є основним документом, який пред΄являється при здачі заліку.

Звіт включає наступні розділи:

1. Титульна сторінка звіту
2. Індивідуальне завдання.
3. Огляд літературних джерел за тематикою, що задана.
4. Теоретичні відомості про метод розв΄язання, його обгрунтування.
5. Програмна реалізація розроблених алгоритмів (виноситься в Додаток).
6. Аналіз результатів, висновки.
7. Перелік джерел посилань.

До звіту додаються щоденник з підписами і печаткою, робоча програма, анотація та відгук керівника від підприємства, зазначається в щоденнику практики.

Оформлюється звіт за вимогами нормативних документів.

Звіт виконується українською мовою без стилістичних, орфографічних і синтаксичних помилок.

Загальний обсяг звіту з виробничої практики не повинен перевищувати 20 сторінок друкованого тексту (шрифт – Time New Roman, розмір – 14, інтервал – 1,5. Береги: верхній – 2 см, нижній – 2 см, лівий – 2,5 см, правий – 1 см).

Звіт друкується з одного боку аркуша білого паперу.

Зміст містить назви та номери початкових сторінок всіх розділів та підрозділів звіту. Текст основної частини звіту поділяють на розділи і підрозділи.

Нумерацію сторінок, розділів, підрозділів, ілюстрацій, таблиць, формул, подають арабськими цифрами без знака №.

Першою сторінкою звіту є титульний аркуш, який включають до загальної нумерації сторінок. На титульному аркуші, першому аркуші змісту номер сторінки не ставлять, на наступних сторінках номер поставляють у правому верхньому куті сторінки без крапки. Нумерація сторінок звіту повинна бути наскрізною: перша сторінка – титульний аркуш, друга – завдання і так далі відповідно до наведених рекомендацій.

Кожну структурну частину звіту треба починати з нової сторінки.

Заголовки структурних частин звіту друкують великими літерами симетрично до тексту (по центру).

***Розділи, підрозділи, пункти, підпункти*** слід нумерувати арабськими цифрами. ***Розділи*** повинні мати порядкову нумерацію в межах викладення суті роботи і позначатися арабськими цифрами без крапки, наприклад 1,2,3,.....і т.д. ***Підрозділи*** нумерують у межах кожного розділу. Номер підрозділу складається з номера розділу і порядкового номера підрозділу, між якими ставиться крапка (наприклад: ”2.3” – третій підрозділ другого розділу). ***Пункти*** нумерують у межах кожного підрозділу, ***підпункти*** – у межах кожного пункту за такими ж правилами (наприклад: ”1.3.2” – другий пункт третього підрозділу першого розділу).

Ілюстрації (схеми, графіки) і таблиці необхідно подавати у роботі безпосередньо після тексту, де вони згадані вперше, або на наступній сторінці. Якщо вони містяться на окремих сторінках звіту, їх включають до загальної нумерації.

Ілюстрації позначають словом Рисунок і нумерують послідовно в межах розділу (наприклад: Рисунок 1.2 – Другий рисунок першого розділу), за винятком ілюстрацій, поданих у додатках. Номер ілюстрації, її назва і пояснювальні підписи розміщують послідовно під ілюстрацією. Назву рисунка друкують з великої літери та розміщують під ним посередині рядка, наприклад,

«**Рисунок 1.2 — Схема устаткування**».

Номер ілюстрації, її назва і пояснювальні підписи (умовні позначки) розміщують безпосередньо під ілюстрацією.

Посилання на ілюстрації в тексті вказують порядковим номером в дужках, наприклад, (Рисунок 1.2), за винятком таблиць, поданих у додатках.

Цифровий матеріал, як правило, оформлюють у вигляді таблиць. ***Таблицю*** слід розміщувати безпосередньо після тексту, в якому вона згадується вперше, або на наступній сторінці. На всі таблиці мають бути посилання в тексті. Нумерують таблиці як і рисунки. Слово „Таблиця” розміщують ліворуч над таблицею. Назву таблиці друкують з великої літери і розміщують над таблицею з абзацного відступу (5 знаків).

Наприклад

Таблиця (номер) - (назва таблиці)

**Таблиця 1.2 – Вихідні дані**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Головка |  |  | |  | | Заголовки колонок |
|  |  |  |  |  | Підзаголовки  колонок |
|  |  |  |  |  |  | Рядки |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Якщо рядки або колонки таблиці виходять за межі формату сторінки, таблицю поділяють на частини, розміщуючи одну частину під іншою або поруч, чи переносять частину таблиці на на­ступну сторінку. У кожній частині таблиці повторюють її головку та боковик. У разі поділу таблиці на частини дозволено її головку чи боковик заміняти відповідно номера­ми колонок або рядків, нумеруючи їх арабськими цифрами в першій частині таблиці.

Слово «Таблиця» подають лише один раз над першою частиною таблиці. Над іншими частинами таблиці з абзацного відступу друкують «Продовження таблиці \_\_\_ » або «Кінець таб­лиці \_\_\_\_» без повторення її назви.

**Формули** та **рівняння** в розташовують безпосередньо після тексту в якому вони згадуються, посередині сторінки з полями зверху та знизу не менше одного рядка. Номер формули або рівняння складається з номера розділу і порядкового номера формули в розділі, між якими ставиться крапка. Номери пишуть біля правого берега аркуша в одному рядку з відповідною формулою в круглих дужках, наприклад: (3.1) (перша формула третього розділу).

Пояснення значень символів і числових коефіцієнтів, що входять до формули або рівняння, слід наводити безпосередньо під формулою у тій послідовності, в якій вони наведені у формулі або рівнянні.

Наприклад:

 (3.1)

де  - математичне очікування;

 – середнє квадратичне відхилення і т.д.;

Формули, що йдуть одна за одною й не розділені текстом, відокремлюють комою.

У звіті додатки мають важливе значення, тому їм необхідно приділити значну увагу. Їх кількість та якість свідчать про те, наскільки студент глибоко вивчив практичні матеріали діяльності підприємства (організації), сумлінно віднісся до збору інформації.

Всі додатки до звіту повинні бути пронумеровані. Посилання у текстовій частин звіту на додатки дається з вказівкою на номер додатку. Кожен із додатків нумеруються у правому верхньому куті і на кожен є посилання у тексті. Додатки повинні позначатися літерами (крім Г; Є; З; І; Ї; Й; О; Ч; Ь), мати заголовок, надрукований з великої літери по центру сторінки.

Виконаний звіт з переддипломної практики переплітають.

**7. Форми та методи контролю**

*Поточний контроль*: індивідуальна практична робота.

*Семестровий контроль:**з*алік.

*Умови допуску до семестрового контролю:*

Обов’язкові:

* Виконані індивідуальний план проходження практики
* Оформлений звітний пакет документів

Необов’язкові:

* Позитивний результат першої атестації та другої атестації.

**8. Критерії оцінювання**

За результатами практики проводиться залік, який відбувається он-лайн за допомогою Zoom чи Meet відкрито перед членами комісії. Атестація за підсумками практики проводиться на підставі письмового звіту, робочої програми та щоденника з практики, оформлених відповідно до встановлених вимог, та відгуку керівника практики у щоденнику практики. Рейтингова оцінка студента за «практику» складається з балів, які він отримує за:

1. виконання індивідуального завдання;

2. підготовка та оформлення звіту;

3. захист звіту з практики.

Система рейтингових (вагових) балів:

|  |
| --- |
|  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № з/п | Контрольний захід | % | Ваговий бал | Кіл-ть | Всього |
| 1. | Виконання індивідуального завдання | 70 | 70 | 1 | 70 |
| 2. | Підготовка та оформлення звіту | 15 | 15 | 1 | 15 |
| 3 | Захист звіту з практики | 15 | 15 | 1 | 15 |
|  | Всього | | | | 100 |

**9. Рекомендована література**

Базова література:

1. Положення про організацію освітнього процесу в КПІ ім. Ігоря Сікорського. – 2020. [Електронний ресурс] – Режим доступу: http://osvita.kpi.ua/node/39

2. Методичні рекомендації з питань організації практики студентів та складання робочих програм практики Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» [Текст] / Уклад.: Н. М. Лапенко, І.Л. Співак, І.В. Федоренко, О.М. Шаповалова; за заг. ред. П.М. Яблонського. – К.: КПІ ім. Ігоря Сікорського, 2018. – 29 с.

3. Головенкін В.П. Інженерна педагогіка (електронне видання): Підручник. – К.: НТУУ «КПІ ім.. Сікорського», 2017. [Електронний ресурс]. – Режим доступу: http://www.kpi.ua/.

4. Головенкін В.П. Педагогіка вищої школи (Андрагогіка): Підручник. – К.: НТУУ «КПІ», 2009. – 406 с.

Додаткова література:

5. Закон України про вищу освіту. Закон від 01.07.2014 № 1556-VII [Електронний ресурс]. – Доступний http://zakon1.rada.gov.ua/laws/show/1556-18

6. Роз’яснення МОН щодо деяких питань практичної реалізації положень нового Закону України «Про вищу освіту» : [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/control/publish/article7art\_icN247526620.

7. Положення про навчання студентів та аспірантів, стажування наукових і науково педагогічних працівників у провідних вищих навчальних закладах та наукових установах за кордоном, затверджене Постановою Кабінету Міністрів України від 13 квітня 2011 року № 411 – [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/411-2011- %D0%BF.

8. Положення про проведення практики студентів вищих навчальних закладів України: Наказ Міністерства освіти України від 8 квітня 1993 р. № 93.

Керівник практики від кафедри ІБ ННФТІ КПІ ім. Ігоря Сікорського

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ доцент Носок С.О.

Керівник практики від підприємства

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(посада, ПІБ, підпис)