# **НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

## “КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

## імені ІГОРЯ СІКОРСЬКОГО”

**НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**

**Кафедра інформаційної безпеки**

|  |  |
| --- | --- |
|  | ЗАТВЕРДЖЕНО |
|  | Вченою радою  НН Фізико-технічного інституту  Директор ННФТІ  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Олексій НОВІКОВ  Протокол № 1 від 16.01.2023 р. |
|  |  |

#### **РОБОЧА ПРОГРАМА ПЕРЕДДИПЛОМНОЇ ПРАКТИКИ**

для здобувачів вищої освіти 4-го курсу спеціальності:

125 «Кібербезпека»

|  |  |
| --- | --- |
|  | Програму рекомендовано кафедрою  інформаційної безпеки |
|  | Протокол № 9 від 15 грудня 2022р. |
|  |  |
|  | Завідувач кафедри інформаційної  безпеки  \_\_\_\_\_\_\_\_ Дмитро ЛАНДЕ |
|  |  |

Київ 2023 р.

**ЗМІСТ**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | |
|  | Вступ…………………………………………………………………..…….. | 3 |
| 1. | Мета і завдання практики………………………………………………… | 5 |
| 2. | Порядок організації, обов’язки керівників та зміст практики…………. | 14 |
| 3. | Календарний план…………………………………………………………. | 23 |
| 4. | Вимоги до звіту……………………………………………………………. | 24 |
| 5. | Форми і методи контролю………………………………………………… | 28 |
| 6. | Критерії оцінювання……………………………………………………….. | 29 |
| 7 | Рекомендована література…………………………………………………. | 31 |
|  |  |  |
|  |  |  |

**ВСТУП**

Переддипломна практика - це практична частина навчального процесу, яка проводиться перед написанням і захистом дипломного проекту.  
Таку практику обов'язково проходять здобувачі вищої освіти, учні або слухачі (виходячи з рівня навчального закладу) при закінченні навчання у ВНЗ, а по завершенню здають звіт з переддипломної практики. Що являє собою переддипломна практика? Така практика являє собою застосування теорії на виробництві після її логічного завершення вивчення в навчальному закладі. Найчастіше переддипломну практику проводять перед захистом і здачею дипломного проекту.

Практика дозволяє здобувачам вищої освіти скористатися теоретичними знаннями, навичками і вміннями, зібрати матеріали для написання і захисту дипломної роботи. У процесі проходження переддипломної практики, майбутні випускники, підбирають всякого роду інформацію про підприємство, на якому вони проходять практику - звітність, баланси, техніко-економічні показники та інші дані.

Після проходження переддипломної практики здобувачі вищої освіти обов'язково складають у письмовому вигляді звіт про її проходження. Як скласти і написати звіт по практиці обов'язково розповість її керівник.

Майбутніми випускниками для проходження практичного переддипломного навчання прийнято вибирати організацію або підприємство, які підходять за профілем діяльності і відповідають спеціалізації навчального закладу майбутнього випускника.

Під час проходження переддипломної практики її учасники можуть користуватися бібліотекою організації або підприємства, отримувати консультації та інформацію від фахівців підприємства. На момент виконання практики здобувачі вищої освіти отримують статус «працівник підприємства» і зобов'язані виконувати і дотримувати вимоги внутрішнього трудового розпорядку підприємства, виробничу дисципліну та охорону праці.

Переддипломна практика є складовою навчального процесу підготовки майбутніх спеціалістів. Переддипломна практика здобувачів вищої освіти останнього курсу проходить на підприємствах, в організація та установах на робочих місцях. Мета практики полягає в тому, щоб здобувач вищої освіти закріпив і поглибив свої теоретичні знання і здобув навички по виконанню виробничих функцій та типових завдань діяльності, якими повинен володіти. У процесі проходження переддипломної практики здобувач вищої освіти повинен ознайомитися зі структурою підприємства, організації чи установи (бази практики), організацією і методами роботи професіоналів за фахом «Кібербезпека». Під час перебування на переддипломній практиці здобувач вищої освіти -практикант збирає матеріали для написання дипломної роботи.

Переддипломна практика здобувачів вищої освіти 4 курсу є невід’ємною частиною освітньо-професійної програми підготовки фахівців, основним завдання якої є якість практичної підготовки випускника за освітньо-кваліфікаційним рівнем бакалавр, та у відповідності до «Положення про проведення практики студентів вищих навчальних закладів України» від 8 квітня 1993р. № 93, «Методичних рекомендацій по складанню програм практики студентів вищих навчальних закладів України» від 14.02.1996 р. № 31-5/197 та навчальних планів спеціальності 125 «Кібербезпека».

Тривалість переддипломної практики у відповідності до Наказу КПІ ім. Ігоря Сікорського №НОН/351/2022 від 22.12.2022 року «Про організацію практики здобувачів вищої освіти у 2023 році» складає 5 тижнів.

Згідно з кваліфікаційною характеристикою бакалавра:

- за фахом «Кібербезпека» спеціалісти отримують знання з математики, інформатики, інформаційної безпеки, кібербезпеки. Професійно орієнтовані дисципліни: основи захисту інформації, захист конфіденційної інформації, математичні методи захисту інформації, теорія інформації та кодування, управління інформаційною безпекою тощо. Вони отримують знання, які дозволяють створювати, нові методи захисту інформації і технології комп’ютерної обробки інформації.

**1 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.

Цілями 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 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.

## 

## 2. ПОРЯДОК ОРГАНІЗАЦІЇ, ОБОВ’ЯЗКИ КЕРІВНИКІВ ТА 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.

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;

- оформити журнал виходу на роботу, а також провести інструктаж з техніки безпеки;

- 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.

**ОБОВ*’*ЯЗКИ**

***Обов’язки відповідального за практику від кафедри***

Основними обов’язками відповідальних за практику від кафедри є:

– своєчасне до початку практики складання наказів про проведення практики та іншої документації на кожного здобувача вищої освіти, з дотриманням встановлених в КПІ ім. Ігоря Сікорського вимог;

* організація та проведення настановних зборів для здобувачів вищої освіти кафедри з метою проведення інструктажу про порядок проходження практики, з техніки безпеки, охорони праці і попередження нещасних випадків та надання їм необхідних документів перед початком практики;

– забезпечення своєчасності отримання здобувачами вищої освіти індивідуальних завдань від безпосередніх керівників;

* своєчасне ознайомлення здобувачів вищої освіти з вимогами до оформлення документації з практики, системою звітності та критеріями оцінки з практики, які регламентуються відповідною нормативною та методичною документацією з організації та проведення практики;

– консультування здобувачів вищої освіти щодо термінів і порядку проходження практики, оформлення документів з практики та захисту звіту;

– своєчасна організація та проведення відкритого захисту практики;

– звітування на засіданні кафедри про підсумки практики;

– своєчасне складання звітів про проведення практики з дотриманням встановлених вимог;

– внесення пропозицій щодо вдосконалення організаційно-методичного забезпечення практики, а також інших навчально-методичних та звітних документів (враховуючи специфіку конкретної спеціальності);

* здійснення, у разі необхідності, разом з науковими керівниками вибіркового контролю за проходженням практики студентами безпосередньо на базі практики.

***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;

– 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;

– організовує і керує науково-дослідною роботою практиканта;

– консультує здобувачів вищої освіти щодо виконання індивідуального завдання практики та оформлення документів з практики;

– своєчасно оцінює роботу здобувача вищої освіти на практиці за результатами звіту з практики, виконання індивідуального завдання та інших документів з практики;

– забезпечує своєчасність надання здобувачами вищої освіти на кафедру звітів з практики та інших документів, необхідних для захисту, їх перевірку та візування;

* здійснює, у разі необхідності, разом з відповідальним за практику 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 відповідальним за практику 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 відповідального за практики від кафедри в разі порушення студентом трудової дисципліни;

– перевіряти звіти про практику, давати письмові характеристики на здобувачів вищої освіти з оцінкою їх ставлення до роботи, дотримання ними трудової дисципліни, рівня теоретичної і практичної підготовки.

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

Зброшурований звіт разом із щоденником студент у визначений кафедрою строк подає відповідальному за практику від кафедри та науковому керівнику.

***Обов’язки практикантів***

Зобов’язані:

– до початку практики на настановних зборах, а далі в індивідуальному порядку, одержати від відповідального за практику консультації щодо проходження практики і оформлення всіх необхідних документів;

– своєчасно прибути на базу практики;

* систематично працювати над виконанням завдань;

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

– у повному обсязі виконувати всі завдання, передбачені програмою практики та вказівками наукового керівника;

– виконувати діючі на підприємстві (в організації) правила внутрішнього розпорядку, строго дотримуватись правил охорони праці, техніки безпеки і виробничої санітарії;

– нести відповідальність за виконану роботу;

– постійно підтримувати контакти з кафедрою та у призначений від повільним за практику від кафедри, або науковим керівником термін з’явитися на проміжний контроль;

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

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

Під час практики здобувач вищої освіти повинен розвинути та закріпити свої навики та вміння:

– проводити бібліографічну роботу із залучення сучасних інформаційних технологій;

– формулювати та реалізувати в практичній площині мету дослідження;

– вибирати необхідні методи дослідження, модифікувати існуючі та розробляти нові методи, виходячи із задач конкретного дослідження;

– проводити наукові дослідження і обробляти отримані результати, аналізувати та осмислювати їх з урахуванням опублікованих матеріалів.

**Рекомендований перелік індивідуальних завдань**

Індивідуальне завдання надає безпосередньо керівник практики від компанії (організації) узгоджуючи з науковим керівником дипломної роботи, індивідуальне завдання повинно бути пов’язане з тематикою дипломної роботи.

1. ChatGPT, як консультант для побудови захищених систем
2. ChatGPT, як консультант для зловмисника для обходу систем захисту
3. Захист системи керування контейнерами Kubernetes
4. Сутність та інфраструктуру об’єктів критичної інфраструктури, їх види (в тому числі найновіші – Розумне місто, Розумний транспорт та ін.) та характерні загрози;
5. Протоколи, які використовуються в складі об’єктів критичної інфраструктури, їх недоліки безпеки , та шляхи вдосконалення;
6. Програмні, програмно-апаратні рішення кіберзахисту об’єктів критичної інфраструктури.
7. Розробка та реалізація політики безпеки на об’єктах критичної інфраструктури, оцінка її дієвості.
8. Методики оцінки ризиків об’єктів критичної інфраструктури;
9. Моделі та сценарії атак та їх виявлення;

10)Поведінковий та психологічний портрет потенційних жертв соціального інженера, сценарії поведінки які призводять до успіху подібних атак;

11) Механізми здійснення різних атак соціальної інженерії;

12) Нові технології та засоби соціальної інженерії, засновані на ML та АІ, в тому числі DeepFake та інші.

13) Рішення кіберзахисту та підходи до попередження атак соціальної інженерії.

14) Загрози безпеці інформації.

15) Сучасний стан законодавчого та нормативно-правового забезпечення захисту інформації.

16) Основні канали витоку мовної інформації та інформації, що передається у телекомунікаційних мережах та системах зв΄язку, методи та засоби її захисту.

17) Закриття мовних сигналів у телефонних каналах, цифрові системи закриття мовних сигналів в каналах зв΄язку.

18) Міжнародні та національні стандарти в галузі взаємодії відкритих систем і систем передачі інформації.

19) Загрози інформації в комп΄ютерних системах.

20) Методологія захисту комп΄ютерних систем.

21) Політика безпеки комп΄ютерних систем, моделі та механізми захисту.

22) Криптографічні засоби захисту інформації.

23) Автентифікація інформації, цифровий підпис.

24) Розробка переборних алгоритмів криптоаналізу класичних шифрів із застосуванням бібліотеки паралельного програмування MPI для кластерної обчислювальної системи.

25) Дослідження та створення бібліотеки отримання фізичних випадкових послідовностей із стандартних засобів обчислювальної техніки.

26) Застосування інфраструктури відкритих ключів.

27) Дослідження незбалансованих фейстелевських схем блокових шифраторів.

28) Дослідження алгебраїчних атак на потокові криптосистеми.

29) Intrusion Detection and Prevention

30) Cyberattack Models and Scenarios

31) NIST Cybersecurity Framework

32) Ransomware Attacks and Scenarios

33) Wireless security protocols

34) Wireless authentication methods

35) Social-engineering attacks, threats, and vulnerabilities

36) Detection of insider actions by anomaly detection

37) Common methods for securing mobile devices

38) Securing Cloud Applications

39) Machine Learning Techniques for Cybersecurity

40) Machine Learning Attack Models

41) Імплементація RBAC, DAC, MAC в хмарних системах

42) Практики забезпечення безпеки процесів неперервної розробки

43) Моделі і автоматизація доступу до середовища контейнерної оркестрації

44) Використання засобів типу Key Vault для міжсервісної автентифікації

45) Автоматизація процесів аудиту політик доступу в хмарних середовищах

46) Визначення аномалій в часових рядах даних без сигнатур та шаблонів

47) Поведінковий аналіз користувачів в мережі

48) Агентне моделювання розповсюдження дезінформації в соціальних мережах

Матеріали, що отримав здобувач вищої освіти під час виконання індивідуального завдання, можуть в подальшому бути використані для виконання кваліфікаційної роботи, для підготовки доповіді, статті або для інших цілей за погодженням з кафедрою і базою практики.

**3 КАЛЕНДАРНИЙ ПЛАН**

З метою успішного здійснення самостійної роботи здобувача вищої освіти необхідно керуватися узагальненим календарним планом переддипломної практики за нижче наведеною формою.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Назва робіт** | **Тижні проходження практики** | | | | | **Примітки**  **про**  **виконання** |
| **1** | **2** | **3** | **4** | **5** |
| **6** | **7** | **8** | **9** | **10** |
| 1. | Проходження інструктажу з ТБ |  |  |  |  |  |  |
| 2. | Остаточне узгодження індивідуального завдання практики з науковим керівником |  |  |  |  |  |  |
| 3. | Проведення експериментальних досліджень |  |  |  |  |  |  |
| 4. | Узагальнення і систематизація отриманих результатів |  |  |  |  |  |  |
| 5. | Оформлення щоденника практики, робочої програми та звіту |  |  |  |  |  |  |

Самостійна робота здобувача вищої освіти передбачає складання й захист звіту про проходження переддипломної практики. Даний звіт повинен мати відомості про виконання всіх розділів програми практики у відповідності до індивідуального плану здобувача вищої освіти. Звіт повинен бути підписаний і оцінений керівником практики. У звіті необхідно подати кількісний та якісний аналіз проведеної роботи. Звіт повинен складатись зі вступу, основної частини, висновків, списку використаних джерел та додатків.

**4 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.

**5 ФОРМИ І МЕТОДИ КОНТРОЛЮ**

***Поточний контроль*:** індивідуальна практична робота.

*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.

***Підсумковий контроль***: це захист звітної документації з практики.

***Семестровий контроль****:**з*алік.

**6 КРИТЕРІЇ ОЦІНЮВАННЯ**

Для оцінювання успішності здобувачів вищої освіти застосовується рейтингова система (РСО), яка враховує:

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 |

При складанні звіту необхідно викладати матеріал у стислій формі. Завдання, процеси і структуру керування викладати у формі схем, таблиць і графіків із застосуванням коротких текстових пояснень. Збір матеріалу для звіту повинен проводитися послідовно і систематично в ході проходження практики у відповідних структурних підрозділах підприємства. Остаточне оформлення звіту і складання висновків проводиться у відведений для цього час. До звіту додаються робоча програма і щоденник практики.

За результатами проходження переддипломної практики здобувач вищої освіти отримує відповідні оцінки (ECTS та традиційних).

|  |  |
| --- | --- |
| **Рейтингові бали** | **Оцінка** |
| 95-100 | «Відмінно» |
| 85-94 | «Дуже добре» |
| 75-84 | «Добре» |
| 65-74 | «Задовільно» |
| 60-64 | «Достатньо» |
| RD ≤ 59 | «Незадовільно» |

Оцінка за практику вноситься в заліково-екзаменаційну відомість і в залікову книжку здобувача вищої освіти та враховується під час визначення стипендії разом з оцінками за результатами підсумкового семестрового контролю.

**7 РЕКОМЕНДАВНА 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. Національна доктрина розвитку освіти України у ХХІ столітті // Освіта України, 2001, № 29.

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