|  |  |  |
| --- | --- | --- |
|  | **https://lh4.googleusercontent.com/_S-0b9ryxRX538VgKXkF1NL439HwkHfdIoR_0jBNAB_tkfTkL84H5-MgDF0HYMschDBOAjqBHgc8hWJBMUUEsKVXPqZh5NGEkbeZnq2C6N6vRcs59oObPRtUrl5aN5hQlCyAQ4b0C3nz** | **НН ФТІ**  **Кафедра інформаційної безпеки** |
| **НАЗВА ДИСЦИПЛІНИ**  **ПО 7 Практика**  **Робоча програма навчальної дисципліни (Силабус)** | | |

# Реквізити навчальної дисципліни

|  |  |
| --- | --- |
| **Рівень вищої освіти** | ***Другий (магістерський)*** |
| **Галузь знань** | *12 Інформаційні технології* |
| **Спеціальність** | *125 Кібербезпека та захист інформації* |
| **Освітня програма** | *«Системи, технології та математичні методи кiбербезпеки»* |
| **Статус дисципліни** | *Нормативна* |
| **Форма навчання** | *Очна (денна)* |
| **Рік підготовки, семестр** | *2 курс, осінній семестр* |
| **Обсяг дисципліни** | *14 кредитів 420 годин* |
| **Семестровий контроль/ контрольні заходи** | *Залік* |
| **Розклад занять** | *http://rozklad.kpi.ua* |
| **Мова викладання** | *Українська* |
| **Інформація про  керівника курсу / викладачів** | Відповідальний: *к.т.н., доцент Носок Світлана Олександрівна*  [*nos.sv.ol@gmail.com*](mailto:nos.sv.ol@gmail.com) |
| **Розміщення курсу** | [*https://ecampus.kpi.ua/login*](https://ecampus.kpi.ua/login) |

# Програма навчальної дисципліни

# Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Програму освітньої компоненти «Переддипломна практика» складено відповідно до освітньо професійної програми «Кібербезпека та захист інформації» підготовки здобувачів вищої освіти спеціальності 125 – Кібербезпека та захист інформації. Дисципліна «Переддипломна практика» є обов’язковим компонентом освітньо-професійної програми підготовки здобувачів вищої освіти другого рівня вищої освіти і має на меті набуття здобувачем вищої освіти необхідних наукових і дослідницьких компетентностей. У програмі переддипломної практики магістрів висвітлюються організаційно-методичні засади практичної професійної підготовки магістрів.

**Мета переддипломної практики.** Переддипломна практика є важливою складовою магістерської програми підготовки інженера-дослідника і має на меті систематизацію, розширення і закріплення професійних знань, формування у магістрів початкової компетенції ведення самостійної наукової роботи, дослідження та експериментування.

Суть переддипломної практики полягає у залученні магістрів 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 та супроводжувальні роботи.

Студент 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 дисципліни** є поглиблення навичок самостійної дослідницької роботи, розширення наукового світогляду магістрів, дослідження проблем практики та вміння пов’язувати їх з обраним теоретичним напрямком дослідження, визначати структуру та логіку майбутньої магістерської роботи.

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

ЗДАТНІСТЬ:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Здатність проводити дослідження на відповідному рівні.

ЗК 3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

ЗК 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

*Фундаментальні компетентності СВО:*

ФК1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, науково-технічні розробки, фізичні та математичні фундаментальні знання і моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у галузі інформаційної безпеки та/або кібербезпеки.

ФК2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ФК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

ФК4.Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

ФК5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення уразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ФК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ФК7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

ФК8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи й засоби захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/ або кібербезпеки організації.

ФК9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

ФК10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

ФК11. Здатність враховувати сучасні міждисциплінарні науково-практичні контексти при прийнятті рішень в галузі інформаційної безпеки та/або кібербезпеки, зокрема, використовуючи апарат аналізу даних та враховуючи вимоги високонавантажених систем.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі результати навчання:

ЗНАННЯ:

РН 1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН 2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах

РН 3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН 5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН 7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН 8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

РН 9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН 10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН 11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН 12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

РН 13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.

РН 14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

РН 15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

РН 16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

РН 17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.

РН 18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

РН 19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності

РН 20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН 21. Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН 22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

РН 23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

РН 24. Мати навички розроблення, впровадження та супроводження проектів з забезпечення інформаційної безпеки та/або кібербезпеки з урахуванням сучасних вимог та принципів побудови високонавантажених систем та аналізу даних.

# Пререквізити та постреквізити дисципліни

Отримані практичні та дослідницькі навички та засвоєні теоретико-методологічні знання під час освоєння навчальної дисципліни «Переддипломна практика» можна використовувати в подальшому для здійснення науково-дослідної діяльності та підготовки магістерської дисертації.

Необхідні навички:

- дисципліна вимагає знань дисциплін з загальної та професійної підготовки: іноземної мови, фізики, математики, програмування, інформаційних технологій, кібербезпеки, теоретичних основ та методології наукових досліджень.

# Зміст навчальної дисципліни

На навчальну дисципліну «Переддипломна практика» відводиться 420 годин / 14 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.

Магістрант 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 студент 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. Магістрант повинен навчитись порядку ведення документації, яка супроводжує наукові дослідження та програмне забезпечення.

Тривалість навчальної дисципліни «Переддипломна практика» – вісім 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;

- 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 магістрантами 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;

- провести інструктаж з техніки безпеки;

- подати до деканату звіт про результати проведення практики.

Підсумки практики обов’язково обговорюються на засіданнях кафедри.

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

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

Магістрантів ознайомлюють із наказом ректора, програмою та завданнями практики, тривалістю робочого часу на практиці, правилами внутрішнього розпорядку та правилами техніки безпеки.

На першому етапі магістранти 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 магістрантами звіту за результатами проходження практики, його захист та залік.

# Навчальні матеріали та ресурси

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. Положення про проведення практики здобувачів вищої освіти КПІ імені Ігоря Сікорського: Наказ Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» від 24.09.2020р. № 7/172.

# Навчальний контент

# Методика опанування навчальної дисципліни (освітнього компонента)

В рамках дисципліни заплановано наступні види навчальних занять: самостійна робота над індивідуальним завданням.

Структура компонентів дисципліни взаємоузгоджена, матеріал вивчається в логічній послідовності. Теми та порядок освоєння дисципліни «Переддипломна практика» наведений нижче.

1. **Практичні заняття**

|  |  |
| --- | --- |
| **№**  **п/п** | **Найменування теми** |
| 1 | **Тема 1. Організація процесу переддипломної практики** |
| 1.1 | 1.1 Настановна конференція |
| 1.2 | 1.2 Інформування магістрантів про мету, завдання і зміст переддипломної практики, місце її проходження |
| 1.3 | 1.3 Ознайомлення студентів з порядком проходження переддипломної практики |
| 1.4. | 1.4 Інструкції щодо виконання робочої програми практики, порядку оформлення всіх необхідних документів, щоденнику практики. |
| 1.5. | Інструктажі з питань охорони праці та техніки безпеки |
| 2 | **Тема 2.** Практична та емпірично-пошукова діяльність |
| 2.1 | 2.1 Пошук та вирішення конкретних наукових проблем; розробка комплексних підходів до її вивчення, обговорення з науковим керівником (керівником практики в організації) |
| 2.2 | 2.2 Проведення експериментальних досліджень, обробка результатів і доведення їх правомірності |
| 2.3 | 2.3 Узагальнення і систематизація отриманих результатів |
| 3 | **Тема 3. Результати переддипломної практики** |
| 3.1 | Підсумкова конференція |
| 3.2 | Підготовка звіту за результатами проходження практики |
| 3.3 | Залікове заняття.Захист звіту за результатами проходження практики |

7.Самостійна робота студента

З метою успішного здійснення самостійної роботи магістранта необхідно керуватися узагальненим календарним планом переддипломної практики за нижче наведеними формами – щоденника практики та індивідуального плану проходження практики.

***Щоденник практики***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№**  **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 магістранта передбачає виконання індивідуального завдання, складання й захист звіту про проходження переддипломної практики. Даний звіт повинен мати відомості про виконання всіх розділів програми практики у відповідності до індивідуального плану магістранта. 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.

***Самостійна робота студента***

|  |  |  |
| --- | --- | --- |
| № з/п | **Вид самостійної роботи** | **Кількість**  **годин СРС** |
| 1. | Виконання індивідуального завдання | 320 |
| 2. | Оформлення звіту та щоденнику | 50 |
| 2. | Підготовка до заліку | 50 |
|  | **Загалом** | **420** |

# Політика та контроль

# Політика навчальної дисципліни (освітнього компонента)

Поточний та підсумковий контроль за виконанням магістрантами програми практики здійснює керівник практики від кафедри.

Щоденник практики є основним документом магістранта під час проходження практики. Під час практики магістрант щодня коротко чорнилом повинен записувати в щоденник усе, що він зробив за день для виконання календарного графіку проходження практики.

У щоденнику в загальній послідовності відображається й діяльність з громадсько-політичної практики. Докладні записи ведуться в робочих зошитах, які є продовженням щоденника. Не рідше, як раз на тиждень, магістрант зобов’язаний подавати щоденник на перегляд керівнику практики, який надає письмові зауваження, додаткові завдання й підписує записи, що їх зробив магістрант. Після закінчення практики щоденник разом із звітом має бути переглянутий керівником практики, який складає відгук й підписує його. Оформлений щоденник разом із звітом магістрант повинен здати на кафедру. Без заповненого щоденника практика не зараховується. Переддипломна практика завершується підсумковою конференцією.

Виведення оцінки за практику для кожного магістранта-практиканта відбувається на заліковому занятті після виконання ним усіх завдань відповідно до плану переддипломної практики.

На залікове заняття кожен магістрант повинен подати пакет звітної документації, який включає:

1. Загальний звіт про проходження практики.

2. Щоденник практики, оформлений належним чином.

Завідувачем кафедри призначається комісія з прийому звітів з практики. Оцінка з практики вноситься в залікову відомість.

**Академічна доброчесність**

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

**Норми етичної поведінки**

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

**Процедура оскарження результатів контрольних заходів**

Студенти мають можливість підняти будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами. Студенти мають право оскаржити результати контрольних заходів, але обов’язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа та/або зауважень.

# Види контролю та рейтингова система оцінювання результатів навчання (РСО)

*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.

*Критерії оцінювання*

Для оцінювання успішності магістрантів застосовується рейтингова система (РСО), яка враховує:

• виконання індивідуального завдання практики;

• підготовку та захист звітної документації.

Система рейтингових (вагових) балів:

|  |
| --- |
|  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № з/п | Контрольний захід | % | Ваговий бал | Кіл-ть | Всього |
| 1. | Виконання індивідуального завдання | 70 | 70 | 1 | 70 |
| 2. | Захист звіту з практики | 30 | 30 | 1 | 30 |
|  | 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 додається щоденник практики.

За результатами проходження переддипломної практики магістрант 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 магістранта та враховується під час визначення стипендії разом з оцінками за результатами підсумкового семестрового контролю.

Підсумки переддипломної практики обговорюються на засіданнях кафедр.

**Робочу програму навчальної дисципліни (Силабус):**

**Складено**:

к.т.н, доцентом Носок Світланою Олександрівною.

**Ухвалено** кафедрою інформаційної безпеки (протокол № 6 від 08.06.2023)

**Погоджено** Методичною комісією ННФТІ (протокол № 6 від 29.06.2023)