Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут
електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

РОБОЧА ПРОГРАМА
Переддипломна практика

ЗАТВЕРДЖУЮ
Завідувачка кафедри
_____ __*Ткач Ю.М.*_____
(підпис) (прізвище та ініціали)
26 серпня 2025р.

Розробник: Петренко Тарас Анатолійович,
доцент кафедри кібербезпеки та математичного моделювання, к.т.н. _____

Робоча програма обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від 26 серпня 2025р. №6

УЗГОДЖЕНО з гарантом освітньої програми: _____ __*Ткач Ю.М.*____
(підпис) (прізвище та ініціали)

Назва курсу	Переддипломна практика
Мова викладання	українська
Викладач	Петренко Тарас Анатолійович, доцент
Профайл викладача	https://mmi.stu.cn.ua/personal-kafedry/ https://scholar.google.com.ua/citations?user=2bJE-4IAAAAJ&hl https://www.linkedin.com/in/taraspetrenko/ https://orcid.org/0000-0001-5571-3815 https://www.webofscience.com/wos/author/record/ABA-8146-2021 https://www.scopus.com/authid/detail.uri?authorId=57193026484
Контакти викладача	тел.: 0504650364, e-mail: mail_taras@ukr.net

1. Анотація курсу. Переддипломна практика є невід'ємною складовою і одним із завершальних етапів у підготовці висококваліфікованих фахівців у сфері кібербезпеки та захисту інформації і має на меті не тільки закріплення теоретичних знань та практичних навичок здобувачами вищої освіти, отриманих ними на етапі навчання, але і проведення досліджень в реальних умовах діяльності підприємств – баз практик, збір необхідних матеріалів для написання магістерської кваліфікаційної роботи. Переддипломна практика – одна з найбільш важливих освітніх компонент підготовки кваліфікованого фахівця з кібербезпеки яка є зв'язуючою ланкою окремих дисциплін з кваліфікаційною роботою магістра та подальшим працевлаштуванням за фахом.

У період практики закладаються основи досвіду професійної діяльності, використання практичних умінь і навичок, професійних якостей особистості майбутнього фахівця з кібербезпеки за освітньо-кваліфікаційним рівнем «магістр». Практика займає важливе місце в вирішенні завдання підготовки висококваліфікованих спеціалістів, які володіють комплексом професійних знань, практичними навичками роботи за спеціальністю 125 Кібербезпека та захист інформації та необхідними організаторськими якостями.

2. Мета та цілі курсу:

– оволодіння здобувачами вищої освіти сучасними методами, навичками, вміннями майбутньої професійної діяльності, формування у них, на базі одержаних в Національному університеті «Чернігівська політехніка» знань, професійних навичок для прийняття самостійних рішень під час роботи в конкретних суспільно-економічних умовах, виховання потреби систематично поповнювати свої знання й творчо їх застосовувати в практичній діяльності.

– закріплення, поглиблення і систематизацію теоретичних знань, отриманих під час навчання за спеціальністю 125 Кібербезпека та захист інформації, в процесі реальної практичної діяльності.

– забезпечення єдності теоретичного і практичного навчання здобувачів вищої освіти з питань організації діяльності підрозділів захисту інформації, включаючи особливості функціонування підприємств та вирішуваних ними завдань, набуття здобувачами вищої освіти практичних навичок розробки пропозицій по вдосконаленню та підвищенню ефективності прийнятих технічних мір і організаційних заходів із застосуванням сучасних технологій захисту інформації, підготовка здобувачів вищої освіти до ефективного використання отриманих знань в процесі самостійного розв’язання фахових завдань. Отримання навичок проведення аналізу інформаційних систем конкретного об'єкту управління з метою самостійного проектування та розробки елементів захищених автоматизованих інформаційних систем з використанням сучасних інформаційних технологій та розвинутих інструментальних засобів захисту інформації.\

Під час проходження переддипломної практики здобувачі вищої освіти розширюють на практиці набуті в ході попереднього навчання наступні загальні та фахові компетентності, передбачені освітньою програмою спеціальності 125 Кібербезпека та захист інформації:

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Здатність проводити дослідження на відповідному рівні.

КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

КЗ6. Здатність до ініціативності, відповідальності та навички до превентивного і аварій-ного планування, управління заходами безпеки професійної діяльності, уміння приймати рішення у складних та непередбачуваних ситуаціях, лідерські якості та знання міжнародних норм і законодавства України у сфері безпеки життєдіяльності населення, системи управління охороною праці та цивільного захисту.

КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і полі-тики інформаційної безпеки та/або кібербезпеки організації.

КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Завдання практики:

– поглиблення, закріплення і поповнення теоретичних знань, придбаних при вивченні навчальних дисциплін за спеціальністю 125 Кібербезпека та захист інформації;

– оволодіння здобувачами вищої освіти сучасними методами, формами організації ро-боти за спеціальністю (практичними навичками з автоматизації захисту інформації, інформаційних систем та процесів, безпечного функціонування автоматизованих інформаційних систем і мереж тощо);

– отримання практичного досвіту роботи за фахом в умовах реальних підприємств та їх структурних підрозділів;

– засвоєння здобувачами вищої освіти на практиці структури інформаційно-аналітичної діяльності та загальнонаукових і спеціальних методів, що застосовуються в управлінні захистом інформації;

– розвиток у здобувачами вищої освіти професійних вмінь приймати самостійні рішен-ня під час виконання конкретної роботи за фахом та ін.

– проведення здобувачами вищої освіти досліджень та збір матеріалів для подальшої підготовки та написання магістерської кваліфікаційної роботи та ін.

3. Результати навчання:

Переддипломна практика надає змогу здобувачам вищої освіти закріпити та поглибити навички передбачені наступними програмними результати навчання:

Переддипломна практика надає змогу здобувачам вищої освіти закріпити та поглибити навички передбачені наступними програмними результати навчання:

ПРН1. 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.

ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних за-дач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

ПРН5. 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.

ПРН15. 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.

ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної без-пеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

ПРН22. 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.

ПРН24. Забезпечувати гарантії збереження здоров'я і працездатності працівників у виробничих умовах через ефективне управління охороною праці та формування відповідальності за колективну та власну безпеку; використовувати методи превентивного та аварійного планування, керувати заходами з безпеки професійної діяльності, приймати рішення у складних та непередбачуваних ситуаціях, вирішувати професійні завдання з урахуванням вимог цивільного захисту та охорони праці.

Після проходження переддипломної практики ЗВО повинні:

знати :

– структуру інформаційно-аналітичної діяльності та загальнонаукових і спеціальних методів, що застосовуються в управлінні захистом інформації;

– існуючі мережні стандарти та протоколи захищеної передачі даних;

– принципи організації безпечної взаємодії між прикладними програмами на різних комп'ютерах в локальних та глобальних мережах;

– особливості виконання організаційної та аналітичної роботи в сфері забезпечення захисту інформації;

вміти:

– робити вибір протоколів та мережевого обладнання, необхідного для забезпечення інформаційної безпеки;

– забезпечувати взаємодію комп'ютерів у мережному середовищі з врахуванням вимог безпеки;

– проводити аналіз умов функціонування підприємства, його розташування на місцевості для визначення можливих джерел загроз;

– досліджувати засоби забезпечення інформаційної діяльності, які мають вихід за межі контрольованої території;

– досліджувати інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання інформації;

– визначати наявність та технічний стан засобів забезпечення технічного захисту інформації;

– виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, кіл і проводів;

– визначати технічні засоби і системи, застосування яких не обґрунтовано службовою чи виробничою необхідністю;

– визначити технічні засоби, що потребують переобладнання та ін.

4. Обсяг курсу. 15 кредитів ECTS, що становить 450 годин самостійної роботи студентів.

Вид заняття	Загальна кількість годин
Самостійна робота (практична діяльність на підприємстві, виконання програми практики та індивідуальних завдання, збір матеріалів до виконання ВКР магістрів)	450

Тематика курсу

1. Ознайомлення з програмою практики. Знайомство з підприємством, його структурою. Інструктаж з техніки безпеки
2. Дослідження підприємства, вивчення його інформаційної діяльності, визначення об`єктів захисту – інформації з обмеженим доступом, технічного обладнання, інформаційно-комунікаційних систем і мереж, виявлення загроз, їх аналіз
3. Аналіз системи забезпечення інформаційної безпеки на підприємстві. (окремо організаційний, технічний, та програмний аспекти) Виявлення слабких місць в системах захисту та уразливостей в інформаційний системі бази практики
4. Розробка рекомендацій щодо вдосконалення системи захисту інформації, підвищення рівня захищеності інформації в інформаційних системах бази практики або практична реалізація і впровадження власної програмної, або інженерно-технічної розробки
5. Виконання індивідуального завдання
6. Підведення підсумків. Узагальнення матеріалів з практики, оформлення звіту, складання диференційного заліку

5. Пререквізити.

Передумовою для проходження переддипломної практики є успішне засвоєння дисциплін передбачених освітньою-професійною програмою Кібербезпека другого (магістерського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації. Дисципліна є базовою для підготовки кваліфікаційної роботи магістра та подальшої успішної професійної діяльності за спеціальністю.

6. Система оцінювання та вимоги

Загальна система оцінювання результатів переддипломної практики	ECTS	Бали
Звітна документація, самостійність, пунктуальність, оформлення	При перевірці та оцінюванні звіту про проходження переддипломної практики враховується повнота правильність виконання завдань передбачених програмою практики, самостійність виконання, терміни здачі та відповідність оформлення звітної документації діючим вимогам. Максимальна кількість балів 30.	30
Індивідуальне завдання	Індивідуальне завдання оцінюється від 0 до 30 балів. Кількість балів залежить від рівня теоретичних знань та практичних навичок студента, самостійності виконання та повноти опрацювання теми індивідуального завдання.	30
Підсумковий контроль	Захист практики. Оцінюються відповіді студентів на питання керівника практика	40

Діяльність ЗВО та форма контролю	Кількість балів	
Якість виконання програми практики та звітної документації	0	10
Самостійність виконання програми практики	0	10
Своєчасність виконання завдань передбачених програмою практики	0	5
Відповідність оформлення звітної документації встановленим критеріям	0	5
Індивідуальне завдання	0	30
Залік (захист практики)	0	40

Шкала оцінювання: національна та ECTS

Критерії оцінювання	Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
Студент виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили, проводить наукові дослідження	90 – 100	**A**	відмінно
Студент вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна	82-89	**B**	добре
Студент вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок	75-81	**C**	
Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих	66-74	**D**	задовільно
Студент володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні	60-65	**E**	
Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу	0-59	**FX**	незадовільно з можливістю повторного складання

7. Політики курсу.

Вивчення курсу базується на принципах взаємної поваги й довіри викладача та здобувача вищої освіти, рівноправності й толерантності.

7.1 Академічна доброчесність - самостійність виконання навчальних завдань та посилання на джерела у випадку використання напрацювань інших авторів. Види порушень академічної доброчесності - академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво.

Відповідно до Кодексу академічної доброчесності Національного університету «Чернігівська політехніка» за порушення академічної доброчесності здобувачі освіти можуть мати наслідком: повторне проходження підсумкового оцінювання; повторне вивчення відповідного освітнього компонента освітньої програми; - відрахування з Університету; позбавлення академічної стипендії.

7.2 Політика дедлайнів - своєчасність здачі практичного завдання оцінюється в 1 бал за кожне завдання. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, відсутність електроенергії чи зв'язку, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом).

7.3 Політика перезарахування кредитів у випадку мобільності - перезарахування кредитів проводиться відповідно до Порядку визначення академічної різниці та визнання результатів попереднього навчання в Національному університеті «Чернігівська політехніка» та Положення про академічну мобільність учасників освітнього процесу Національного університету «Чернігівська політехніка»

7.4 Політика щодо відвідування - відвідування занять є обов'язковим. При наявності поважних причин (хвороба, участь в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом) студенти можуть узгодити з викладачем індивідуальний графік навчання та здачі всіх видів навчальної роботи. Студенти можуть перескладати або відпрацьовувати пропущені заняття на консультаціях викладача чи у спеціально відведений викладачем для цього час.

Здобувач вищої освіти, який має більше 30% пропусків навчальних занять (без поважних причин) від загального обсягу аудиторних годин згідно з індивідуальним начальним планом не допускається до складання екзамену під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому Положенням про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка»

7.5 Політика щодо правил поведінки на заняттях - активна участь у навчальному процесі, виконання необхідного мінімуму навчальної роботи, коректна поведінка щодо інших учасників навчального процесу, взаємоповага, використання мобільних пристроїв та комп'ютерної техніки тільки для навчання.

7.6 Політика заохочень та стягнень. Результати навчальної, наукової та організаційної діяльності студентів за напрямами курсу їм можуть нараховуватися додаткові бали - до 10 балів, в залежності від вагомості досягнень студента. Види позанавчальної діяльності, за які студенти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, статті на науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

7.7. Політика оскарження результатів контрольних заходів. Для вирішення спірних питань, пов'язаних із організацією та проведенням семестрового контролю, оцінювання практик, атестації та визнанні результатів навчання в неформальній та/або інформальній освіті на факультеті створюється апеляційна комісія розпорядженням декана, до складу якої включаються, завідувачі кафедр, науково-педагогічні працівники та представники органів студентського самоврядування. Головою апеляційної комісії призначається декан. Порядок подання та розгляду апеляцій визначається відповідно до р.7 Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка».

8. Рекомендована література та інформаційні джерела

1. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006.

2. Про вищу освіту [Текст]: Закон України № 1556-VII від 01.07.2014 // Відомості Верховної Ради, 2014, № 37-38, ст. 2004.

3. Правила забезпечення захисту інформації в інформаційних телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою КМУ від 29 березня 2006. - №373.

3. Положення про проведення практики здобувачів вищої освіти Національного університету «Чернігівська політехніка» затверджено Вченою радою Національного університету «Чернігівська політехніка» 31 серпня 2020 р. протокол № 6 Введено в дію наказом ректора від 31 серпня 2020 р. № 26

4. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання: ДСТУ ГОСТ 7.1:2006. Чинний від 07.01.2007. - К. : Держспоживстандарт України, 2007. - 47 с.

5. Система дистанційного навчання НУ «Чернігівська політехніка». – [Електронний ресурс]. – Режим доступу: https://eln.stu.cn.ua/course/view.php?id=4413

6. Центр розвитку кар'єри.– [Електронний ресурс]. – Режим доступу: http://robota-chntu.stu.cn.ua/

7. Державна служба спеціального зв'язку та захисту інформації України. – [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua