ЗАТВЕРДЖЕНО

Вченою радою
факультету інформаційно-
комп'ютерних технологій
31 серпня 2023 р., протокол № 5

Голова Вченої ради
Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА ПРАКТИКИ
ОК 15 «ПЕРЕДДИПЛОМНА ПРАКТИКА»

для здобувачів вищої освіти освітнього ступеня «магістр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної
інженерії та кібербезпеки
28 серпня 2023 р., протокол № 7

Завідувач кафедри
Андрій ЄФІМЕНКО

Гарант освітньо-
професійної програми
Володимир ВОРОТНІКОВ

Розробник: доктор технічних наук, доцент, професор кафедри комп'ютерної інженерії та кібербезпеки Володимир ВОРОТНІКОВ

Житомир
2023 – 2024 н.р.

1. Опис освітньої компоненти

Переддипломна практика магістрів є обов'язковим компонентом освітньо-професійної програми для здобуття кваліфікаційного рівня магістр зі спеціальності 125 «Кібербезпека та захист інформації» і має на меті набуття студентом професійних навичок та вмінь здійснення самостійної науково-дослідної та професійної роботи.

Проходження переддипломної практики є найважливішою частиною й невід'ємним етапом для формування кваліфікованого й професійно компетентного фахівця. Професійна компетентність формується на основі синтезу теорії й практики й проявляється в стані актуалізації здатності особистості не тільки розв’язувати фахові задачі, а й висувати й вирішувати професійні проблеми. Особливу значимість на етапі професійної підготовки майбутнього фахівця здобуває проблема включення студентів у процес практичного оволодіння професійною діяльністю та придбання навичок вирішення комплексних професійних проблем.

Переддипломна практика магістрантів є підсумковим етапом навчання і представляє собою проведення системного аналізу забезпечення об′єкта дослідження методами та засобами кібербезпеки.

Суть переддипломної практики полягає у залученні магістрантів до самостійної роботи, ознайомленні з організацією роботи на підприємствах, збір матеріалів для магістерської роботи.

Предметом практики є поглиблення навичок самостійної роботи та розширення наукового світогляду магістрантів; вивчення проблем практики та вміння пов’язувати їх з обраним теоретичним напрямком дослідження; отримання досвіду визначати структуру і логіку майбутньої професійної роботи фахівця відповідної кваліфікації.

Переддипломна практика дає магістранту реальну можливість систематизувати отримані знання і направити їх на вирішення проектних та науково-дослідних завдань. Практика проводиться в установах, організаціях і підприємствах різних організаційно-правових форм та різних сфер діяльності. Основною вимогою до місця проходження практики є відповідність спеціальності магістранта профілю діяльності підприємства (або окремого підрозділу). Бази практики визначаються в залежності від тематики магістерських робіт (дисертацій) та відповідають необхідним вимогам програми практики.

Характеристика освітньої компоненти

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів 6</td><td>Галузь знань
12 Інформаційні технології</td><td colspan="2">нормативна
(нормативна, за вибором)</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність
125 Кібербезпека та захист інформації</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 1</td><td>2-й</td><td>2-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин - 180</td><td>3-й</td><td>3-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми навчання: аудиторних самостійної роботи – 180</td><td rowspan="11">Освітній ступінь
«Магістр»</td><td>год.</td><td>год.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>год.</td><td>год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>год.</td><td>–</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>180 год.</td><td>180 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td colspan="2">Диференційований залік</td></tr>
</table>

2. Мета і завдання переддипломної практики

Метою переддипломної практики є систематизація та поглиблення теоретичних знань магістрантів з дисциплін спеціальності «Кібербезпека та захист інформації», отримання навичок проведення аналізу сучасної системи захисту конкретного об'єкта з метою самостійного моделювання можливих кіберзагроз та розроблення плану кіберзахисту, уточнення предмету, мети та завдань наукового дослідження згідно теми магістерської дипломної роботи.

Основними ***завданнями*** переддипломної практики є:

збір матеріалів за темою магістерської роботи, вивчення нових досягнень, огляд існуючих рішень виявленої та сформульованої проблеми, вироблення методично правильної системи виконання досліджень і впровадження отриманих результатів;

вироблення навиків творчого підходу до вирішення теоретичних і практичних задач проектування, конструювання, створення і випробування

елементів і систем захисту інформації;

вивчення на практиці сучасних методів несанкціонованого доступу та захисту інформації від стороннього впливу;

аналіз існуючих засобів захисту передачі інформації по технічним каналам інформаційно-комунікаційних систем;

отримання досвіду оцінювання головних техніко-економічних показників у відповідності до чинних нормативно-технічних документів;

вивчення заходів з техніки безпеки, охорони праці, протипожежної безпеки та охорони навколишнього середовища.

Під час практики поглиблюються і закріплюються теоретичні знання магістрантів з усіх дисциплін навчального плану; підбираються фактичні дані та інші матеріали, які використовуються з метою вивчення об`єкта дослідження і пов`язуються з питаннями магістерської роботи. Переддипломна практика є завершальною в циклі практичної підготовки магістра до самостійної професійної діяльності.

Зміст переддипломної практики направлений на формування ***компетентностей***, визначених стандартом вищої освіти зі спеціальності 125 «Кібербезпека»:

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

КЗ-2. Здатність проводити дослідження на відповідному рівні.

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

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

КФ-1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ-2. 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 у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

КФ-3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

КФ-4. 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.

КФ-5. 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 політики інформаційної безпеки та/або кібербезпеки організації.

КФ-6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ-7. 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.

КФ-8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ-9. 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.

КФ-10. 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.

Отримані знання і практичний досвід під час переддипломної практики стануть складовими наступних **результатів навчання** за спеціальністю 125 «Кібербезпека та захист інформації»:

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.

РН-4. 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.

3. Зміст переддипломної практики

Зміст переддипломної практики визначається темою магістерської дипломної роботи і відображається в індивідуальному плані. Магістрант під час проходження переддипломної практики зобов'язаний: повністю виконати завдання, передбачені програмою практики; виконувати правила внутрішнього розпорядку на підприємстві; пройти інструктаж і дотримуватися правил охорони праці та техніки безпеки; нести відповідальність за виконану роботу на підприємстві (за дорученням керівника практики) нарівні зі штатними співробітниками; вести щоденник практики за етапами її проходження; подати на кафедру письмовий звіт про виконання переддипломної практики та індивідуального завдання разом із відгуком, підписаним керівником (куратором) практики від підприємства; захистити основні положення, відображені у звіті.

Перелік основних видів робіт та термінів виконання подано в таблиці.

№ п/п	Зміст роботи	Кількість годин
1	Загальне ознайомлення з підприємством бази практики. Опис напрямків діяльності.	8
2	Техніка безпеки та охорона праці у підрозділах підприємства бази практики.	4
3	Призначення, принципи та особливості роботи призначеного структурного підрозділу бази практики.	6
4	Аналіз технічних каналів інформаційно-комунікаційної системи об'єкта управління, матеріальних та інформаційних потоків, їх взаємодія. Вивчення процесів збирання, зберігання та оброблення даних у межах структурного підрозділу. Призначення, структура і порядок використання застосовуваних апаратних і програмних засобів.	60
5	Аналіз стану системи безпеки об'єкта управління. Ознайомлення з існуючими методами реалізації несанкціонованого доступу (НСД) та методами захисту інформації від стороннього впливу.	60
6	Розробка вимог щодо захисту інформації від НСД та пропозицій щодо необхідних засобів захисту інформації в інформаційно-комунікаційній системі об'єкта управління.	30
7	Оформлення звіту з практики.	12
8	Всього	180

4. Порядок організації проведення практики

Переддипломна практика може проводитися в державних, муніципальних, громадських, комерційних і некомерційних організаціях чи підприємствах, де можливий збір і вивчення матеріалів, пов'язаних із виконанням магістерської

роботи, а також у навчальних та наукових підрозділах університету за напрямом підготовки студентів.

Організація практики на всіх етапах спрямована на забезпечення безперервності і послідовності оволодіння студентами навичками та вміннями професійної діяльності відповідно до вимог згідно з рівнем підготовки магістра. Практика проводиться відповідно до індивідуальної програми переддипломної практики, узгодженою студентом та науковим керівником на основі загальних підходів до її змісту та структури.

Перед початком практики проводяться консультаційні збори, на яких надається вся необхідна інформація з порядку проведення переддипломної практики та інструктаж з техніки безпеки. За результатами зборів студенти заповнюють щоденники, в яких наводять таке: відомості про себе, назву бази практики, вид практики, період проходження практики, календарний графік із переліком запланованих до виконання робіт. Календарний графік студенти завіряють підписом керівника від університету, підписом декану факультету та печаткою факультету. За необхідності студентом на базу практики надається направлення від університету.

На першому тижні практики студент повинен: отримати завдання для проходження переддипломної практики; узгодити графік консультацій зі своїм керівником на кафедрі та ознайомитися з графіком відвідувань даної бази практики; завірити підписом календарний графік у завідувача кафедри (для тих, хто проходить практику на кафедрі), або у керівника іншої бази практики (для тих, хто проходить практику за межами університету); завірити підписом та печаткою керівництва бази практики прибуття студента на практику; пройти інструктаж із техніки безпеки на базі практики.

На останньому тижні практики студент повинен: після закінчення терміну проходження практики за результатами виконаних робіт оформити робочі записи у щоденнику та отримати відгуки керівника від кафедри та керівника від бази практики; завірити підписом та печаткою керівництва бази практики вибуття студента з практики; сформувати звіт, титульний аркуш якого підписати з боку студента, керівника від університету та керівника від бази практики; якщо базою практики не є університет, то на підпис керівника від бази практики поставити печатку підприємства (організації, установи). Індивідуальний план переддипломної практики студента повинен бути узгоджений з планом роботи організації, що є базою практики. У період практики студенти підкоряються всім правилам внутрішнього розпорядку і техніки безпеки, встановленим у підрозділі і на робочих місцях.

5. Керівництво та контроль проходження практики

Керівництво практикою здійснюється кафедрою «Комп'ютерної інженерії та кібербезпеки». Для проходження практики для всіх студентів визначаються куратори від бази практики, під керівництвом яких студенти виконують поставлені в програмі завдання. Керівник переддипломної практики від кафедри надає студенту організаційне сприяння та методичну допомогу у вирішенні завдань.

За виконанням програми практики здійснюється двосторонній контроль з боку керівників від кафедри та бази практики.

Керівник від кафедри контролює роботу магістрантів, аналізує хід виконання програми практики, а в кінці практики перевіряє оформлені студентом щоденник та звіт, приймає участь у роботі комісії по прийому диференційованого заліку.

Керівник практики від підприємства регулярно контролює хід виконання основних видів робіт за планом практики та індивідуальних завдань. З метою забезпечення ефективної роботи практикантів проводить лекційні заняття для висвітлення питань, включених до програми практики, та здійснює аналіз конкретних виробничих ситуацій. В кінці практики перевіряє й підписує звіт про практику, складає характеристику-відзив на кожного магістранта.

6. Звітність та оцінювання результатів практики

За результатами переддипломної практики магістрант надає на кафедру:

щоденник переддипломної практики студента;

розгорнутий звіт про результати переддипломної практики, який складається з титульного аркуша, завдання на практику, змісту, вступу, основної частини, висновків (самостійної оцінки роботи), списку використаної літератури та, при необхідності, додатків;

презентацію та текст підготовленої доповіді за матеріалами переддипломної практики.

Рекомендуєма структура і зміст звіту:

вступ - визначити суть та актуальність проблеми дослідження і указати шляхи її вирішення за рахунок удосконалення системи інформаційної безпеки;

перший розділ - описати сферу діяльності бази практики та її інформаційні потоки, які підлягають захисту;

другий розділ - проаналізувати систему захисту об′єкта управління;

третій розділ - провести огляд і аналіз існуючих методів захисту

інформації та їх реалізацію, а також проаналізувати засоби захисту інформації в інформаційно-комунікативних системах;

висновки - визначити недоліки та проблеми існуючої системи захисту інформації на об′єкті управління.

Атестацію за підсумками практики проводять на підставі захисту результатів, отриманих у ході переддипломної практики.

Магістрант звітується комісії, яку призначає завідувач кафедри. До захисту студент подає звіт з практики та щоденник, підписаний керівником від бази практики, з відзивом і оцінкою.

За результатами звіту комісія диференційовано оцінює роботу магістранта. Оцінка за практику вноситься в залікову-екзаменаційну відомість та в залікову книжку студента і в подальшому враховується стипендіальною комісією при визначенні розміру стипендії.

Студент, який не виконав програму практики, або отримав незадовільну оцінку, залишається на повторний курс навчання або відраховується з університету. Результати проведення практики обговорюються на засіданні кафедри.

Шкала оцінювання

За шкалою	Диференційований залік	Бали
A	Відмінно	90-100
B	Добре	82-89
C		74-81
D	Задовільно	64-73
E		60-63
FX	Незадовільно	35-59
F		0-34

7. Рекомендована література

Основна література

1. Стандарт вищої освіти України: другий (магістерський) рівень, галузь знань 12 Інформаційні технології, спеціальність 125 Кібербезпека. Затверджено і введено в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.
2. ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. – Київ: ДП ″УкрНДНЦ″, 2016. – 17 с.
3. ДСТУ 3008-15 Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Київ: ДП ″УкрНДНЦ″, 2016. – 31 с.

4. ДСТУ 1.5:2015 Національна стандартизація. Правила розроблення, викладання та оформлення нормативних документів. – Київ: ДП ″УкрНДНЦ″, 2015. – 65 с.
5. Вимоги до оформлення курсових і дипломних проектів: методичні рекомендації для студентів галузі знань 12 ″Інформаційні технології″ / уклад. А. А. Гаврилова, С. П. Євсеєв, Г. П. Коц, О. Г. Руденко. – Харків: ХНЕУ ім. С. Кузнеця, 2018. – 50 с.
6. Данильян О. Г. Дзьобань О. П. Методологія наукових досліджень: підручник – Харків: Право, 2019. – 368 с.

Допоміжна література

7. Закон України “Про національну безпеку (2018).
8. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015).
9. Закон України “Про захист персональних даних” (2010).
10. Наскрізна програма практики для студентів спеціальності 125 "Кібербезпека" другого (магістерського) рівня [Електронний ресурс] / уклад. С. П. Євсеєв, О. В. Мілов, О. Г. Король. – Харків: ХНЕУ ім. С. Кузнеця, 2021. – 32 с.
11. Чмиленко Ф.О., Жук Л.П. Посібник до вивчення дисципліни «Методологія та організація наукових досліджень» – Дніпро: РВВ ДНУ, 2014. – 48 с.
12. Методологія і організація наукових досліджень. [текст]: навч. посіб. / Г.О. Бірта, Ю.Г. Бургу– Київ: «Центр учбової літератури», 2014. – 142с.

8. Інформаційні ресурси мережі Інтернет

1. Освітній портал: https://learn.ztu.edu.ua/ .
2. Бібліотечно-інформаційний ресурс Житомирської обласної універсальної наукової бібліотеки ім. Олега Ольжича (http://www.lib.zt.ua/, 10014, м. Житомир, Новий бульвар, (0412) 37-84-33), Національної бібліотеки України ім. В.І. Вернадського (http://www.nbuv.gov.ua/, Київ, просп. Голосіївський, 3, +380 (44) 525-81-04) та ін.