ПРОГРАМА
науково-дослідної практики

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***другий (магістерський)***
Освітня програма	***Кібербезпека***

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 2 від 31.08.2020 р.

Розробник:
Євсеєв С. П., д.т.н., проф. кафедри КІТ.
Мілов О.В., к.т.н., проф кафедри КІТ.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

ВСТУП

Магістр - освітньо-кваліфікаційний рівень вищої освіти особи, яка на основі освітньо-кваліфікаційного рівня бакалавра здобула повну вищу освіту, спеціальні уміння та знання, достатні для виконання професійних завдань та обов'язків (робіт) інноваційного характеру відповідного рівня професійної діяльності, що передбачені для первинних посад у різних сферах діяльності.

Науково-дослідна практика магістрів є обов'язковим компонентом освітньо-професійної програми для здобуття кваліфікаційного рівня магістра з відповідної спеціальності і має на меті набуття студентом професійних навичок та вмінь здійснення самостійної науководослідної та педагогічної роботи.

Методичні вказівки призначені для організації та проведення науково- дослідної практики магістранта другого року навчання факультету економічної інформатики за спеціальністю125 “Кібербезпека”. Для студента-магістранта важливо не тільки знати основні положення, характерні для магістерської дипломної роботи, але мати загальне уявлення про методологію наукової творчості, здобути досвід у організації своєї роботи, у використанні методів наукового пізнання та застосуванні логічних законів і правил. У даних методичних вказівках розглядаються загальні питання організації, проведення і підведення підсумків науково-дослідної практики студентів

Предметом науково-дослідної практики є поглиблення навичок самостійної наукової роботи, розширення наукового світогляду студентів, дослідження проблем практики та вміння пов’язувати їх з обраним теоретичним напрямком дослідження, визначати структуру та логіку майбутньої магістерської роботи.

Характеристика навчальної дисципліни

Курс	**1**
Семестр	**2**
Кількість кредитів ECTS	**2**
Форма підсумкового контролю	ЗВІТ

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
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	ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-20 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
СК 1. Здатність розробляти та впроваджувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти з метою	ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства).

здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	
СК 3. Здатність розробляти й впроваджувати систему менеджменту інформаційної безпеки та/або кібербезпеки організації, формувати стратегію і політики інформаційної безпеки різних рівнів на базі світових й вітчизняних стандартів з урахуванням кращих практик галузі інформаційних технологій та їх безпеки.	ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат; ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства); ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо); ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки.
СК 9. Здатність розробляти та впроваджувати методи і заходи протидії кіберінцидентам, а також здійснювати процедури управління, контролю та розслідування, надавати рекомендації щодо попередження та аналізу кіберінцидентів.	ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо).
СК 11. Здатність розробляти, впроваджувати і супроводжувати системи аудиту та моніторингу якості бізнес/операційних процесів інформаційно-комунікаційних систем та технологій, а також системи менеджменту інформаційної безпеки та/або кібербезпеки організації в цілому.	ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства); ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; ПРН-15 – розробляти, впроваджувати та супроводжувати процеси

	управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки.
СК 12. Здатність проводити науково-освітню діяльність, розробляти та впроваджувати систему управління персоналом, а також проводити та планувати навчання працівників і наукові дослідження в сфері безпеки інформаційно-комунікаційних систем і технологій у відповідність вітчизняним та світовим стандартам галузі інформаційної безпеки та/або кібербезпеки	ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат; ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки; ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому; ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо); ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства); ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації

	користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки; ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства); ПРН-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на підприємстві.

2. МЕТА І ЗАВДАННЯ НАУКОВО-ДОСЛІДНОЇ ПРАКТИКИ

Метою науково-дослідної практики є систематизація, розширення професійних знань у сфері обраної спеціальності, формування і розвиток в студентів-магістрантів навичок до самостійної наукової праці, проведення досліджень і експериментів, закріплення отриманих теоретичних знань за дисциплінами напрямку і спеціальним дисциплінам магістерських програм.

Основним завданням практики є набуття досвіду в дослідженні актуальної наукової проблеми, а також підбір необхідних матеріалів для виконання випускної кваліфікаційної роботи – магістерського дипломного проекту.

Науково - дослідна практика є завершальною в циклі практичного становлення студентів.

Під час науково-дослідної практики студент повинен вивчити:

- патентні й літературні джерела з метою їхнього використання при виконанні випускної кваліфікаційної роботи;
- методи дослідження й проведення експериментальних робіт;
- методи аналізу й обробки експериментальних даних;
- фізичні й математичні моделі процесів й явищ, що стосуються об'єкта, що досліджується;
- інформаційні технології в наукових дослідженнях, програмні продукти, що належать до професійної сфери;
- вимоги до оформлення науково-технічної документації; виконати:
- аналіз, систематизацію й узагальнення науково-технічної інформації за темою досліджень;
- теоретичні або експериментальні дослідження в рамках поставлених завдань, включаючи математичний (імітаційний) експеримент;
- аналіз вірогідності отриманих результатів;
- порівнювати результати досліджень об'єкта розробки з вітчизняними й закордонними аналогами;
- аналіз наукової й практичної значимості проведених досліджень, а також техніко-економічної ефективності розробки.

За час науково-дослідної практики студент повинен в остаточному вигляді сформулювати тему магістерської дипломної роботи й обґрунтувати доцільність її розробки.

3. БАЗИ ПРАКТИКИ

Основним базовим об’єктом науково-дослідної практики є кафедра кібербезпеки та інформаційних технологій, а також на договірних засадах у державних, муніципальних, суспільних, комерційних і некомерційних організаціях, підприємствах і установах, що здійснюють функції кібербезпеки на яких можливе вивчення й збір матеріалів, пов'язаних з виконанням випускної кваліфікаційної роботи.

Перед початком практики проводиться вступна консультація, на якій дається вся необхідна інформація із проведення науково-дослідної практики.

Для проходження практики для всіх магістрантів призначаються викладачі - куратори від кафедри, а також куратори від бази практики, під керівництвом яких магістранти проходять практику у виробничих колективах.

Індивідуальна програма діяльності студента повинна бути погоджена з планом роботи колективу бази практики й обумовлена цілями й завданнями науково-дослідної практики.

У підрозділах, де проходить практика, студентам виділяються робочі місця для виконання індивідуальних завдань по програмі практики.

У період практики студенти підкоряються всім правилам внутрішнього розпорядку й техніки безпеки, установленим у підрозділі й на робочих місцях.

По закінченню практики студенти оформляють усю необхідну документацію відповідно до вимог програми практики.

4. ПОРЯДОК ОРГАНІЗАЦІЇ ТА КЕРІВНИЦТВО НАУКОВО-ДОСЛІДНОЇ ПРАКТИКОЮ

Науково-дослідна практика для студентів магістратури проводиться згідно з навчальним планом кафедри кібербезпеки та інформаційних технологій для студентів денної форм навчання. Протягом проходження науково-дослідної практики та виконання основних завдань програми практики, кожен студент повинен отримати конкретні наукові результати з обраної наукової проблеми, що будуть відображені у формулюванні теми випускної роботи магістра.

Програма науково-дослідної практики студентів магістратури складається з наступних частин:

- формування індивідуального графіку проходження науково-дослідної практики та ознайомлення студента з вітчизняними та іноземними науковими та іншими джерелами літератури з метою формування студентом бібліографічного списку літератури за обраним напрямом дослідження. За цей період студенти зобов’язані здійснити огляд нормативної документації та друкованої літератури, зібрати та обробити практичний та інформаційний матеріал, здійснити підбір та обробку статистичних даних з обраного напряму магістерської роботи,
- підготовка рецензії на наукову статтю з обраної проблеми досліджень, а також на основі опрацювання нормативної бази та виявлених недоліків їх практичного застосування готують рекомендації до відповідних органів влади і управління з метою підвищення ефективності вирішення назрілих проблем;
-підготовка тез для виступу на науковій конференції за обраним напрямом. У цей же період студенти готують оглядову наукову статтю за обраним напрямом досліджень з дотриманням вимог ВАКУ. (Друк статті – бажаний).
- виконання індивідуального завдання, завершення роботи над формуванням теми магістерської роботи, оформлення звіту про проходження науково-дослідної практики і захищають його.

Навчально-методичне керівництво і виконання програм практик забезпечуються кафедрою. Загальну організацію практики та контроль за її проведенням на факультеті здійснює керівник практик кафедри кібербезпеки та інформаційних технологій.

Для безпосереднього керівництва практикою кожного студента кафедра призначає наукового керівника з числа викладачів тільки з науковим ступенем доктора або кандидата

наук, який, як правило, поєднує ці обов'язки з обов'язками наукового керівника кваліфікаційної роботи студента. Робота безпосереднього наукового керівника входить до педагогічного навантаження, обсяг якого визначається з діючими нормативами.

Розпочинаючи проходження практики, студент повинен завчасно отримати інструктаж з практики на кафедрі.

Основними обов’язками відповідальних за науково-дослідну практику від кафедри є:

– організація та проведення настановчої конференції для студентів кафедри та надання їм необхідних документів перед початком практики;

– забезпечення своєчасності формування студентами індивідуальних графіків проходження практики

– своєчасне проведення установчих зборів з науково-дослідної практики, ознайомлення студентів 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 студентів щодо термінів і порядку проходження практики, оформлення документів з практики та захисту звіту;

– забезпечення своєчасності надання студентами на кафедру звітів з науково-дослідної практики та інших документів, необхідних для захисту, їх перевірка та візування;

– звітування на засіданні кафедри про підсумки практики;

– розробка та надання студентам індивідуальних завдань та інших вказівок для проходження практики;

– контроль за своєчасністю формування та виконанням індивідуальних графіків проходження практики студентами;

– консультування студентів щодо виконання індивідуального завдання практики та оформлення документів з практики;

– своєчасне оформлення відгуку і попередня оцінка роботи студента на практиці на підставі перевірки звіту з практики, результатів виконання індивідуального завдання та інших документів з практики;

– здійснення, у разі необхідності, разом з керівником-організатором практики від кафедри, вибіркового контролю за проходженням практики студентами безпосередньо на базі практики.

Обов’язки студентів-практикантів

Студенти при проходженні науково-дослідної практики зобов’язані:

– до початку практики на настановних зборах, а далі в індивідуальному порядку, одержати від керівника практики консультації щодо оформлення всіх необхідних документів;

– систематично працювати над виконанням завдань за програмою практики,

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

– висвітлити результати виконаної роботи та оформити їх у звіті про проходження практики;

– своєчасно надати на кафедру звітні документи та у належний термін захистити матеріали практики.

5. ЗМІСТ ПРАКТИКИ

Науково-дослідна практика здійснюється у формі проведення реального дослідницького проекту, виконуваного студентом у рамках затвердженої теми наукового дослідження з напрямку навчання й теми магістерської роботи з урахуванням інтересів і можливостей підрозділів, у яких вона проводиться.

Тема дослідницького проекту може бути визначена як самостійна частина науково-дослідної роботи, виконуваної в рамках наукового напрямку випускаючої кафедри

«Кібербезпеки та інформаційних технологій».

Зміст практики визначається керівником програми підготовки магістрів й відбивається в індивідуальному завданні на науково-дослідну практику.

Робота магістрантів у період практики організовується відповідно до логіки роботи над магістерською роботою: вибір теми, визначення проблеми, об'єкта й предмета дослідження; формулювання мети й завдань дослідження; теоретичний аналіз літератури й досліджень по проблемі, добір необхідних джерел по темі (патентні матеріали, наукові звіти, технічна документація й ін.); складання бібліографії; формулювання робочої гіпотези; вибір бази проведення дослідження; визначення комплексу методів дослідження; проведення експерименту; аналіз експериментальних даних; оформлення результатів дослідження. Магістранти працюють із першоджерелами, монографіями, авторефератами й дисертаційними дослідженнями, консультуються з науковим керівником і викладачами.

За час практики студент повинен сформулювати в остаточному виді тему магістерської роботи по профілю свого напрямку підготовки із числа актуальних наукових проблем, розроблювальних у підрозділі, і погодити її з керівником програми підготовки магістрів.

Важливою складовою змісту науково-дослідної практики є збір і обробка фактичного матеріалу й статистичних даних, аналіз відповідних до теми характеристик організації, де студент магістратури проходить практику й збирається впроваджувати або апробувати отримані в магістерській роботі результати.

Діяльність студента на базі практики передбачає кілька етапів:

Етап 1 - Дослідження теоретичних проблем у рамках програми магістерської підготовки:

- вибір і обґрунтування теми дослідження;
- складання робочого плану й графіка виконання дослідження;
- проведення дослідження (постановка мети і конкретних завдань, формулювання робочої гіпотези, узагальнення й критичний аналіз праць вітчизняних і закордонних фахівців з теми дослідження);
- складання бібліографії по темі науково-дослідної роботи.

Етап 2 - Дослідження об'єкту контролю відповідно до теми магістерської роботи:

- опис об'єкта й предмета дослідження;
- збір і аналіз інформації про предмет дослідження;
- вивчення окремих аспектів розглянутої проблеми;
- аналіз процесу контролю;
- статистична й математична обробка інформації;
- аналіз наукової літератури з використанням різних методик доступу до інформації: відвідування бібліотек, робота в Інтернет.
- оформлення результатів проведеного дослідження і їх узгодження з науковим керівником магістерської проекту.

Етап 3- Заключний етап.

Даний етап є останнім етапом практики, на якому магістрант узагальнює зібраний матеріал відповідно до програми практики; визначає його достатність і вірогідність.

Очікувані результати від науково-дослідної практики наступні:

- знання основних положень методології наукового дослідження й уміння застосувати їх при роботі над обраною темою магістерської дисертації;
- уміння використовувати сучасні методи збору, аналізу й обробки наукової інформації;
- уміння викласти наукові знання по проблемі дослідження у вигляді звітів, публікацій доповідей.

За підсумками практики студент надає на кафедру:

- список бібліографії по темі магістерської дисертації;
- письмовий звіт у вигляді першого розділу магістерської дисертації (або реферат по теоретичній частині);
- текст підготовленої статті (доповіді) по темі дисертації.
- звіт по практиці, завізований науковим керівником, представляється керівникові програми підготовки магістрів.

5. Керівництво й контроль над проходженням практики

Керівництво й контроль над проходженням практики покладають наказом декана на керівника практики по напрямку підготовки.

Загальне учбово-методичне керівництво практикою здійснюється випускаючою кафедрою приладів та систем орієнтації та навігації.

Кафедра виділяє керівника науково-дослідної практики, який виявляє магістрантові організаційне сприяння й методичну допомогу в рішенні завдань виконуваного дослідження.

Керівник практики:

- погоджує програму науково-дослідної практики й тему дослідницького проекту з науковим керівником програми підготовки магістрів;
- проводить необхідні організаційні заходи щодо виконання програми практики;
- визначає загальну схему виконання дослідження, графік проведення практики, режим роботи студента й здійснює систематичний контроль над ходом практики й роботи студентів;
- надає допомогу студентам із усіх питань, пов'язаних із проходженням практики й оформленням звіту.

Науковий керівник:

- здійснює постановку завдань по самостійній роботі студентів у період практики з видачею індивідуального завдання по збору необхідних матеріалів для написання магістерської дисертації, надає відповідну консультаційну допомогу;
- дає рекомендації з вивчення спеціальної літератури й методів дослідження;
- бере участь у роботі комісії із захисту дослідницького проекту.

Студент-магістрант:

- проводить дослідження із затвердженої теми відповідно до графіка практики й режимом роботи підрозділу - місця проходження практики;
- одержує від керівника практики вказівки, рекомендації й роз'яснення із усіх питань, пов'язаним з організацією й проходженням практики;
- звітує про виконану роботу відповідно до встановленого графіка.

6. ФОРМИ І МЕТОДИ КОНТРОЛЮ

На місцях проходження практики регламент робочого дня студентів має відповідати внутрішньому розпорядку, установленому для персоналу організації - бази практики, і є обов'язковим для студентів.

Робота практиканта з виконання програми практики контролюється науковим керівником. Практикант повинен дотримуватися режиму роботи та правил внутрішнього розпорядку. Спізнення на заняття та порушення графіку навчального процесу у зв’язку з проходженням практики студентом не припускається.

Виконання кожного розділу практики завіряється підписом керівників практики. По закінченні практики науковий керівник готує відгук на виконання програми практики.

7. ПІДВЕДЕННЯ ПІДСУМКІВ ПРАКТИКИ

Атестація за підсумками практики проводиться на підставі захисту оформленого звіту й відгуку керівника або куратора практики у комісії, що включає наукового керівника магістерської програми, наукового керівника магістранта й керівника практики по напрямкові підготовки. За підсумками позитивної атестації студентові виставляється диференційована оцінка (відмінно, добре, задовільно).

Оцінка по практиці прирівнюється до оцінок по дисциплінах теоретичного навчання й ураховується при проведенні підсумків проміжної (сесійної) атестації студентів.

За результатами науково-дослідної практики студенти представляють до друку підготовлені ними статті, готовлять виступи на наукові й науково-практичні конференції й семінари.

У результаті проходження практики студент повинен:

- володіти навичками самостійного планування й проведення наукових досліджень, що вимагають глибокої підготовки у відповідному напрямку приладів і систем орієнтації та навігації;
- формулювати й вирішувати завдання, що виникають у ході науково-дослідної діяльності й потребують поглиблених професійних знань в області приладів і систем орієнтації та навігації;
- вибирати необхідні методи досліджень, модифікувати існуючі й розробляти нові методи, виходячи із завдань конкретного дослідження;
- обробляти отримані результати, аналізувати й осмислювати їх з урахуванням даних, наявних у літературі;
- вести бібліографічну роботу із залученням сучасних інформаційних технологій;
- представляти підсумки виконаної роботи, отримані в результаті проходження практики, у вигляді рефератів (огляд літератури), статей, оформлених відповідно до наявних вимог, із залученням сучасних засобів редагування й друку;
- володіти методами презентації наукових результатів на наукових семінарах і конференціях із залученням сучасних технічних засобів

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Великий тлумачний словник української мови / уклад. і голов. ред. В. Т. Бусел. – Київ; Ірпінь : Перун, 2009. – 1736 с.

2. 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.

3. ДСТУ 7093:2009 Бібліографічний запис. скорочення слів і словосполук, поданих іноземними європейськими мовами. – Київ : Кн. палата України, 2017. – 17 с.

4. ДСТУ 3582:2013 Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила. – Київ: Мінекономрозвитку України, 2014. – 15 с.

5. ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. – Київ : ДП ″УкрНДНЦ″, 2016. – 17 с.

6. ДСТУ 3008-15 Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Київ : ДП ″УкрНДНЦ″, 2016. – 31 с.

7. ДСТУ 3651.0-97 Метрологія. Основні одиниці фізичних величин Міжнародної системи одиниць. Основні положення, назви та позначення. – Київ : ДП ″УкрНДНЦ″, 1997. – 14 с.

8. ДСТУ 1.5:2015 Національна стандартизація. Правила розроблення, викладання та оформлення нормативних документів. – Київ : ДП ″УкрНДНЦ″, 2015. – 65 с.

9. Женченко М. Загальна і спеціальна бібліографія: навч. посіб. / М. Женченко. – Київ : Жнець, 2011. – 255 с.

10. Основные стандарты для современного книгоиздательского дела / Рос. кн. палата ; сост. : А. А. Джиго,. С. Ю. Калинин, Г. П. Калинина. – Київ: М. Сухоруков, 2008. – 656 с.

11. Про затвердження Вимог до оформлення дисертації: Наказ від 12.01.2017 р. № 40 [Електронний ресурс] // База даних ″Законодавство України″ / ВР України. – Режим доступу до журн. : http://zakon2.rada.gov.ua/laws/show/z0155-17/print1509912703741 483 (дата звернення: 10.04.2018).

12. Словник книгознавчих термінів / уклад.: В. Я. Буран, В. М. Медведєва, Г. І. Ковальчук, М. І. Сенченко. – Київ : Аратта, 2003. – 160 с.

13. Отенко І. П. Основи наукових досліджень : конспект лекцій / І. П. Отенко. – Х. : ХНЕУ, 2010. – 79 с.

14. Пушкар О. І. Основи наукових досліджень. Конспект лекцій для студентів спеціальності 7.050109 усіх форм навчання / О. І. Пушкар, О. А. Єрмоленко. – Х. : Вид ХНЕУ, 2005. – 88 с.

15. Пушкарь А. И. Основы научных исследований и организация научно-исследовательской деятельности : учеб. пособ. / А. И. Пушкарь, Л. В. Потрашкова. – Х. : Изд. ИНЖЕК, 2006. – 289 с.

Додаткова

16. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (1994);

17. Закон України "Про захист персональних даних" (2010)

18. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015)

19. Закон України "Про національну безпеку (2018)

20. ISO/IEC 27001. "Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью.

21. ISO/IEC 27002. "Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью."

22. ISO/IEC 27005. "Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности