

Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка



«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи

Олексій ЖИЛЬЦОВ
2023 р.

ПРОГРАМА ПРАКТИКИ
«НАУКОВО-ДОСЛІДНИЦЬКА ПРАКТИКА»

для студентів

спеціальності	125 Кібербезпека та захист інформації
освітнього рівня	другого (магістерського)
освітньої програми	125.00.02 Безпека інформаційних і комунікаційних систем



2023 – 2024 навчальний рік

Розробники:

Соколов Володимир Юрійович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка, гарант освітньої програми 125.00.02 Безпека інформаційних і комунікаційних систем.

Срмошин Валерій Віталійович, директор департаменту ПрАТ «Національна енергетична компанія Укренерго».

Романюк Олександр Миколайович, здобувач другого (магістерського) рівня освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем.

Складанний Павло Миколайович, кандидат технічних наук, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Коршун Наталія Володимирівна, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

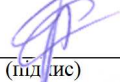
Програму практики розглянуто і затверджено на засіданні Вченої ради Факультету інформаційних технологій та математики

Протокол від 19.10.2022 р. № 1

Секретар  Світлана СЕМЕНЯКА
(підпис)

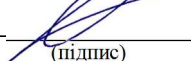
Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 01.09.2022 р. № 12

Завідувач кафедри  Павло СКЛАДАННИЙ
(підпис)


Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.02 Безпека інформаційних і комунікаційних систем)

____.____. 2022 р.

Керівник освітньої програми  Володимир СОКОЛОВ
(підпис)

Програму практики перевірено

____.____. 2022 р.

Заступник декана  Євген ІВАНІЧЕНКО
(підпис)

Пролонговано:

на 2023/2024 н.р.  (підпис)  (ПІБ), «23» 08 2023 р., протокол № 8

на 20__/20__ н.р. _____ (підпис) _____ (ПІБ), «____» ____ 20__ р., протокол № ____

на 20__/20__ н.р. _____ (підпис) _____ (ПІБ), «____» ____ 20__ р., протокол № ____

на 20__/20__ н.р. _____ (підпис) _____ (ПІБ), «____» ____ 20__ р., протокол № ____

1. Опис практики

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид практики	науково-дослідницька	
Загальний обсяг кредитів / годин	4,5/135	
Курс	2	
Семестр	3	
Кількість змістових компонентів з розподілом	3	
Обсяг кредитів	4,5	
Обсяг годин, в тому числі:	135	
Тривалість (у тижнях)	3	
Форма семестрового контролю	залік	

2. Базы практики

Науково-дослідницька практика проводиться на підприємствах, в організаціях, науково-дослідницьких та інших установах, що спеціалізуються на наданні послуг в сфері інформаційних технологій та інформаційної безпеки, банках, страхових компаніях, компаніях-операторах зв'язку та інших, що мають у складі своєї структури підрозділ, що відповідає за інформаційну безпеку, або в будь-яких організаціях, де використовуються технічні засоби обробки, зберігання та передачі конфіденційної інформації.

Закріплення баз практики повинно сприяти встановленню та зміцненню довгострокових контактів університету з підприємствами, а також розвитку кооперації між ними з метою якісної підготовки фахівців. Визначенню баз практик повинна передувати постійна робота кафедри щодо вивчення виробничих та економічних можливостей підприємств з точки зору придатності їх для проведення практики студентів за спеціальністю. При цьому повинні враховуватись перспективи сучасних напрямів розвитку ІТ-галузі, економічного, соціального та екологічного розвитку суспільства.

До підприємств - баз науково-дослідницької практики висуваються такі вимоги:

здійснення діяльності дослідження, проектування, впровадження і експлуатація програмних засобів;

наявність високого рівня технічного забезпечення, використання сучасних інформаційних та інтелектуальних технологій;

забезпечення проходження практики невеликими групами студентів.

Базы практики повинні мати високий рівень техніки та технологій, використовувати сучасну обчислювальну техніку та інформаційні технології; забезпечувати можливість проведення науково-дослідницької практики з дотриманням програми; мати науково-технічні зв'язки з закладом вищої освіти (ЗВО).

Орієнтовний перелік баз практики

1. Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України

2. Інститут проблем математичних машин і систем Національної академії наук України

3. Інститут програмних систем Національної академії наук України

4. Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка

Вибір баз практики здійснюється кафедрою інформаційної та кібернетичної безпеки з урахуванням завдань практики та можливостей їх реалізації. Студенти можуть самостійно, з дозволу кафедри, підбирати для себе місце проходження практики та пропонувати його для використання.

3. Мета і завдання практики

Практична підготовка студентів є важливою складовою сучасного освітнього процесу та спрямована на оволодіння студентами системою професійних вмінь і навичок. Практика формує первинний досвід професійної діяльності та сприяє успішному саморозвитку студента. Така форма практичної підготовки фахівця покликана не тільки забезпечити набуття професійних компетентностей, а також суттєво впливає на формування важливих рис особистості спеціаліста.

Мета науково-дослідницької практики – формування у випускника професійних практичних навичок, необхідних для роботи на підприємствах, застосування отриманих професійних знань, поглиблення та закріплення теоретичних положень з фахових дисциплін, завершення формування бази фактичних знань для виконання магістерської роботи.

Проходження науково-дослідницької практики має на меті:

- вивчення джерел за темою, що розробляється, з метою їх використання при розробці магістерської роботи;
- вивчення методів дослідження та проведення експериментальних робіт, методів аналізу та обробки експериментальних даних;
- вивчення моделей процесів та явищ, що присутні в об'єкті дослідження;
- виконання теоретичного або експериментального дослідження в рамках поставлених задач;
- аналіз, систематизацію та узагальнення науково-технічної інформації за темою досліджень;
- поглиблення та закріплення теоретичних знань з фахових дисциплін;
- вивчення вимог до оформлення науково-технічної документації.

Завдання полягають у формуванні наступних компетентностей:

ЗК 1 Здатність застосовувати знання у практичних ситуаціях.

ЗК 2 Здатність проводити дослідження на відповідному рівні.

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).

ЗК 6 Здатність до професійного спілкування іноземною мовою

ФК 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.

ФК 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.

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

ФК 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.

ФК 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.

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

ФК 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.

ФК 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.

ФК 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.

ФК 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.

ФК(У) 11 Здатність до застосування сучасних безпекових інформаційних та SMART-технологій у сфері захисту інформації.

ФК(У) 12 Здатність до виявлення уразливостей та забезпечення безпеки телекомунікаційних технологій і SMART-інфраструктури. розслідування інцидентів інформаційної та/або кібербезпеки та протидії зловиякісному програмному забезпеченню.

4. Результати проходження практики

В результаті проходження науково-дослідницької практики студент повинен досягти наступних програмних результатів навчання:

РН 3 Проводити 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 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(У) 24 Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях та SMART -інфраструктурі. Вміти проектувати захищені (з урахуванням загроз) проводові і безпроводові телекомунікаційні та SMART -системи.

5. Структура практики

№ з/п	Етапи проходження практики та види діяльності студентів	Усього годин
Етап 1. Організаційний етап. Розробка планів і ознайомлення зі змістом практики		
1	Участь в установчій конференції	2
2	Організаційні заходи щодо проходження практики, ознайомлення з програмою, завданнями, формами звітності з практики	3
3	Розробка планів і визначення змісту практики	5
	Разом	10
Етап II. Виконання завдань за планом практики		
4	Виконання програми науково-дослідницької практики за індивідуальним планом	115
	Разом	115
Етап III. Підсумки науково-дослідницької практики		
5	Підготовка звітних матеріалів про проходження практики	5
6	Участь в звітній конференції.	5
	Разом	10

6. Зміст практики

Етап 1. Організаційний етап науково-дослідницької практики

Організаційні заходи щодо проходження науково-дослідницької практики

Визначення баз проходження практики. Закріплення студентів за базами практики та науковими керівниками практики. Проведення організаційних заходів щодо проходження науково-дослідницької практики. Проведення установчої конференції. Розробка методичних рекомендацій та індивідуальних завдань на проходження практики з урахуванням особливостей баз практики.

Складання індивідуальних планів проходження науково-дослідницької практики

Знайомство з базами практики та уточнення індивідуальних завдань на проходження практики. Розробка плану проходження практики та узгодження його з керівниками баз практики. Складання індивідуальних планів проходження практики. Затвердження індивідуальних планів проходження практики.

Етап 2. Виконання програми науково-дослідницької практики

Виконання програми науково-дослідницької практики

Збір, систематизація й узагальнення теоретичного, методичного та практичного матеріалу за темою магістерської роботи. Розроблення та обґрунтування конкретних практичних положень, що можуть бути використані у магістерській роботі. Звіт перед науковим керівником за результатами першої половини науково-дослідницької практики.

Етап 3. Заключний етап науково-дослідницької практики

Підготовка до захисту і захист звітних матеріалів про проходження практики

Оформлення комплекту звітних матеріалів про проходження практики. Затвердження результатів практики науковим керівником. Підготовка до захисту і захист звітних матеріалів про проходження практики. Обговорення результатів практики на звітній конференції. Підведення підсумків практики. Проведення заліку.

6.1 Особливості організації та проведення практики

Науково-дослідницька практика передбачає безперервність та послідовність її проведення, формування у студентів необхідного і достатнього обсягу практичних знань і вмінь відповідно до освітнього ступеня магістра. Як частина основної освітньої програми є завершальним етапом навчання і проводиться після засвоєння студентом програм теоретичного і практичного навчання. На цій практиці студент всебічно вивчає один із напрямів діяльності освітніх установ, виконує індивідуальні завдання, збирає практичний і статистичний матеріал та створює теоретичну та експериментальну базу для якісного виконання магістерської роботи та її захисту.

Завданням практики є також набуття навичок, умінь і знань планування, підготовки, організації і виконання науково-дослідної роботи, а також оформлення її результатів. Це досягається шляхом вивчення і узагальнення літературних джерел за темою магістерської роботи, підготовки матеріальної бази для її виконання, оволодіння технікою і методикою експериментальних досліджень, отримання попередніх експериментальних даних за темою магістерської роботи, розробки алгоритму її подальшого виконання, грамотного оформлення звіту з практики. Наступний публічний захист звіту з практики дозволяє студенту продемонструвати вміння і здатність викладати результати своєї роботи і відстоювати сформульовані ним наукові положення.

Зміст науково-дослідницької практики визначається індивідуальним планом проходження науково-дослідницької практики, що розробляється студентом разом з науковим керівником магістерської роботи і затверджується на засіданні випускової кафедри. Індивідуальний план має бути тісно пов'язаним з темою магістерської роботи й передбачати систематичну звітність про проходження практики перед науковим керівником.

Основними напрямками діяльності студента під час науково-дослідницької практики мають бути:

- робота по збору й обробці теоретичних і методичних матеріалів, що стосуються магістерської роботи;

- систематизація й обробка практичного матеріалу за темою магістерської роботи, у тому числі з використанням сучасних технологій збору інформації, обробки та інтерпретації отриманих експериментальних та емпіричних даних та сучасних методів досліджень;

- розробка і обґрунтування практичних рекомендацій, що можуть бути наслідком виконання магістерської роботи. Рекомендації повинні мати теоретичний, методичний та практичний характер, стосуватись теми магістерської роботи, грамотно сформульовані й письмово оформлені;

- специфіка обраної теми магістерської роботи може припускати апробацію розроблених рекомендацій.

Керівник магістерської роботи разом із керівником науково-дослідницької практики від кафедри надає всебічну консультативну допомогу практиканту, здійснює загальний контроль підготовлених студентами навчально-методичних матеріалів, контактує з керівництвом бази практики, де проходять практику студенти-практиканти.

Забезпечення якісного проведення науково-дослідницької практики передбачає виконання певних організаційних заходів, таких як:

- обґрунтоване визначення бази практики;
- розподіл студентів за базами практики з урахуванням їх потреб і тематики магістерських робіт;
- складання оптимальних індивідуальних планів проходження науково-дослідницької практики з урахуванням здібностей і схильностей студентів;
- розроблення необхідного навчально-методичного забезпечення науково-дослідницької практики;
- проведення установчої і звітної науково-практичної конференції за участю наукових керівників практики і викладачів випускової кафедри.

6.2. Завдання для самостійної роботи та перелік індивідуальних завдань для студентів

Індивідуальне завдання є однією з форм набуття фахових компетентностей, яка має на меті поглиблення, узагальнення та закріплення знань, які студенти отримали у процесі теоретичного навчання, та застосування цих знань в практичній діяльності.

Напрями і тематика індивідуальних завдань для студентів-практикантів розробляються на випусковій кафедрі, виходячи з теми і завдань магістерської роботи, схильностей, здібностей, особливостей студентів та їх уподобань.

Індивідуальне завдання є особистим для кожного студента, визначається керівником практики спільно з керівником магістерської атестаційної роботи та виконується у відповідності до її тематики. Індивідуальні завдання виконують студенти самостійно у супроводженні керівника практики. Як правило, індивідуальні завдання виконуються окремо кожним студентом. У тих випадках, коли завдання мають комплексний характер, до їх виконання можуть залучатися кілька студентів.

Приклади індивідуальних завдань на науково-дослідницьку практику:

1. Дослідження методик оцінки захищеності систем інформаційної безпеки.
2. Дослідження моделі адаптивної системи інформаційної безпеки.
3. Дослідження показників захищеності системи інформаційної безпеки.
4. Моделювання системи захисту інформації.
5. Дослідження методики застосування інструментальних засобів для аналізу системи захисту інформації.
6. Моделювання процесів захисту інформації в інтегрованих системах безпеки.
7. Дослідження абстрактних моделей контролю доступу до захищених режимом обробки інформації.
8. Дослідження моделей і методів рольового і сесійного контролю доступу.
9. Математичне моделювання загроз безпеці.
10. Моделювання вразливостей реалізації і атак.
11. Моделювання загроз атак з відкладеною реалізацією.

12. Моделювання надійнісних параметрів і характеристик безпеки.
13. Математичне моделювання потенційного порушника.
14. Дослідження експлуатаційних характеристик безпеки.
15. Моделювання реалізованості загроз атак на інформаційну систему.
16. Формування вимог для систем захисту інформації базового рівня захисту.
17. Формування вимог для систем захисту інформації підвищеного рівня захисту.
18. Оцінка ефективності структурного резервування для підвищення безпеки інформаційних систем.

6.3. Обов'язки студентів під час проходження практики

Студенти при проходженні науково-дослідницької практики зобов'язані:

- до початку практики одержати від керівника практики консультації щодо її проходження і оформлення всіх необхідних документів;
- у повному обсязі виконувати всі завдання, передбачені програмою науково-дослідницької практики та індивідуальним планом;
- вести календарно-тематичний план проходження практики, своєчасно оформити всі документи з практики і скласти залік;
- проходити практику за строками, визначеними у наказі по Університету;
- суворо дотримуватись правил охорони праці, техніки безпеки і виробничої санітарії.

6.4. Обов'язки керівників практики від Університету та від бази практики

Керівник науково-дослідницької практики від Університету:

- розподіляє разом із завідувачем випускової кафедри магістрантів на місця проходження практики;
- надає методичні рекомендації щодо складання індивідуальних планів проходження практики магістрантами і затверджує їх після погодження з завідувачем випускової кафедри;
- забезпечує постійне керівництво та контроль за виконанням індивідуального плану кожним магістрантом і надає необхідну допомогу;
- надає консультації практикантам щодо виконання індивідуальних завдань і робочої програми практики;
- контролює виконання магістрантами правил внутрішнього трудового розпорядку, облік відвідування магістрантами практики;
- повідомляє магістранта про систему звітності з практики;
- підводить підсумки науково-дослідницької практики магістрантів, оцінює роботу кожного студента, складає рецензії за результатами проведеної ним практики і надає його завідувачу випускової кафедри.

Керівник науково-дослідницької практики від підприємства:

- організує проходження практики закріплених за ним студентів спільно з керівником від Університету;
- ознайомлює студентів з організацією праці на конкретному робочому місці;
- здійснює контроль за роботою практикантів, допомагає виконувати завдання на даному робочому місці, надає консультації щодо виробничих питань;
- контролює ведення щоденників та складає на кожного студента характеристику-відгук керівника практики від підприємства, який
- заноситься до відповідного розділу щоденника науково-дослідницької практики;
- ознайомлюється зі звітом студента та дає оцінку звіту і роботі студента.

7. Контроль навчальних досягнень

7.1 Система оцінювання навчальних досягнень студентів

Навчальні досягнення студентів з науково-дослідницької практики оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практиці, за виконання індивідуальних завдань, за самостійну роботу. Модульний контроль здійснюється після виконання завдань практики студентами за відповідним змістовим модулем.

№ з/п	Види робіт/діяльності студента	Форма звітності	Максимальна кількість балів		
			За одиницю	Кількість одиниць	Максимальна кількість балів
1	Складання індивідуального плану практики	план	20	1	20
2	Виконання програми науково-дослідницької практики	робочі матеріали	100	1	100
3	Оформлення звітних матеріалів	звіт	40	1	40
			Разом	-	160
Захист практики:					30
Максимальна кількість балів					190
Розрахунок коефіцієнта: $k=190/100=1,9$					

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *методи усного контролю: індивідуальне опитування, фронтальне опитування, співбесіда, залік;*
- *методи письмового контролю: реферат, звіт;*
- *комп'ютерного контролю: тестові програми;*
- *методи самоконтролю: уміння самостійно оцінювати свої знання, самоаналіз.*

Кількість балів за виконання завдань практики, індивідуальних завдань, самостійної роботи залежить від дотримання таких вимог:

- *систематичність відвідування бази практики за індивідуальним планом роботи;*
- *своєчасність виконання навчальних та індивідуальних завдань;*
- *повний обсяг їх виконання;*
- *якість виконання навчальних та індивідуальних завдань;*
- *самостійність виконання;*
- *творчий підхід до виконання завдань;*
- *ініціативність у виконанні завдань практики.*

7.2 Перелік звітної документації

На захист звіту про проходження науково-дослідницької практики студент повинен надати наступні звітні матеріали:

- 1) Індивідуальний план проходження науково-дослідницької практики з позначками про виконання/невиконання його пунктів.
- 2) Календарно-тематичний план проходження практики.
- 3) Звіт про виконання індивідуального завдання.
- 4) Відгук керівника практики про результати і якість проходження студентом науково-дослідницької практики.

Студент, який не надав звітної документації, вважається таким, що не пройшов науково-дослідницьку практику.

7.3 Вимоги до звіту про практику

Після закінчення терміну науково-дослідницької практики студенти звітують про виконання програми та індивідуальних завдань. Звіт має містити відомості про виконання усіх розділів індивідуального плану проходження науково-дослідницької практики та індивідуального завдання, мати висновки і пропозиції, список використаних джерел тощо. Оформлюється звіт за вимогами, які встановлені на кафедрі інформаційної та кібернетичної безпеки.

Звіт про проходження науково-дослідницької практики захищається студентом у комісії, призначеній завідувачем кафедри. До складу комісії входять керівники практики від університету і, за можливості, від бази практики. За результатами захисту і наявності повного комплексу звітних матеріалів виставляється оцінка за науково-дослідницьку практику, яка заноситься до залікової відомості і до залікової книжки студента. Підсумки науково-дослідницької практики підводяться на звітній конференції.

7.4 Шкала відповідності оцінок

Систему рейтингових балів для різних видів контролю та порядок їх переведення у європейську (ECTS) шкалу подано нижче у таблиці.

Шкала оцінювання ECTS

Сума балів за всі види навчальної діяльності	Оцінка за шкалою ECTS	Значення оцінки
90-100	A	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
82-89	B	Дуже добре – достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
75-81	C	Добре – в цілому добрий рівень знань (умінь) з незначною кількістю помилок
69-74	D	Задовільно – посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
60-68	E	Достатньо – мінімально можливий допустимий рівень знань (умінь)
35-59	FX	Незадовільно з можливістю повторного складання – незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
1-34	F	Незадовільно з обов'язковим повторним вивченням курсу – досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

8. Рекомендовані джерела

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В.Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний, Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178 с

2. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.
3. Закон України «Про інформацію» від 02.10.1992 № 2657-ХІІ
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
5. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373
6. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
7. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
8. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
9. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу
10. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
11. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2
12. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу
13. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
14. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу
15. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

ДОДАТКИ

Зразок оформлення Щоденника навчальної практики студента
Титульна сторінка

Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

ЩОДЕННИК ПРАКТИКИ

студента _____

(прізвище, ім'я та по батькові)

Курс _____

Група _____

Спеціальність: 125 «Кібербезпека»

Освітній рівень: другий (магістерський)

Київ – 2022

Друга і наступні сторінки Щоденника**Календарний графік проходження практики**

№ з/п	Назви робіт	Тижні проходження практики	Відмітки про виконання
1	2	3	4

Керівники практики:

від Університету

(підпис) (прізвище та ініціали)

Робочі записи під час практики

Продовження Додатку А

Висновок керівника практики від Університету про проходження практики

Дата складання заліку „_____” _____ 20____ року

Оцінка:
за національною шкалою _____

кількість балів _____

за шкалою ECTS _____

Керівник практики від Університету

(підпис)

(прізвище та ініціали)

Відгук керівника практики від Університету про роботу студента

ПІБ студента повністю

1. Актуальність і практичне значення виконуваної роботи.
2. Позитивні сторони у роботі.
3. Недоліки або дискусійні питання у роботі.
4. Якість та повнота оформлення звіту з навчальної практики.
5. Оцінка особистих якостей студента та отриманих практичних навичок.
6. Загальна оцінка практики.

Зразок оформлення першої сторінки звіту про проходження практики

Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

ЗВІТ**про проходження науково-дослідницької практики**

студента _____
(прізвище, ім'я, по батькові)

групи _____

спеціальність: 125 «Кібербезпека»

Освітній рівень: другий (магістерський)

Керівник практики від Університету _____
(посада, прізвище, ініціали)

Звіт захищений з оцінкою _____ *(підпис керівника практики від Університету)*
«_____» _____ 20_ р.