МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

МЕТОДИЧНІ ВКАЗІВКИ

до проведення науково-дослідницької практики

для студентів денної форми навчання другого (магістерського) рівня вищої освіти за спеціальністю 125 (F5) “Кібербезпека та захист інформації”

Затверджено
редакційно-видавничою
радою університету,
протокол № 3 від 30.10.2025 р.

Харків
НТУ “ХПІ”
2025

Методичні вказівки до проведення науково-дослідницької практики для студентів денної форми навчання другого (магістерського) рівня вищої освіти за спеціальністю 125 (F5) “Кібербезпека та захист інформації” / уклад. О. Г. Король, С. В. Мілевський, А. А. Гаврилова. – Харків: НТУ “ХПІ”, 2025 – 36 с.

Укладачі: О. Г. Король,
С. В. Мілевський,
А. А. Гаврилова

Рецензент Д.А. Кудій

Кафедра кібербезпеки

ВСТУП

Науково-дослідницька практика для студентів денної форми навчання другого (магістерського) рівня навчання за спеціальністю 125 (F5) “Кібербезпека та захист інформації” за науково-дослідницька практика за освітньо-науковою програмою “Кібербезпека” входить до складу базових дисциплін. Вони повинні проходити у строки, які встановлені в графіках навчального процесу, та виступають ключовими етапами у їх підготовці. Проведення науково-дослідницької практики має вирішальне значення для магістрів із кібербезпеки, оскільки вона виступає містком між академічною освітою та науково-професійною діяльністю.

Науково-дослідницька практика за **освітньо-науковою програмою** “Кібербезпека” не лише спрямована на закріплення теоретичних знань та набуття практичних навичок, а й на проведення *самостійного наукового дослідження*, результати якого стануть основою для магістерської кваліфікаційної роботи.

Практика дає можливість застосувати знання, отримані під час навчання, для вирішення реальних завдань у сфері кібербезпеки. Студенти не просто вивчають концепції, а вчаться застосовувати їх, наприклад, під час проведення пентестів, аудиту безпеки чи реагування на інциденти. Це дозволяє їм зрозуміти, як функціонують захищені системи та які виклики виникають у реальному світі.

При проходженні практики відбувається формування ключових фахових компетентностей, які неможливо повноцінно здобути в аудиторії, до складу яких входять: аналітичні навички: вміння аналізувати вразливості, виявляти загрози та оцінювати ризики для конкретної інфраструктури; навички роботи з інструментами: освоєння професійного програмного забезпечення та обладнання, що використовується для моніторингу, захисту й аналізу безпеки; м'які навички (soft skills): робота в команді, ефективна комунікація з колегами та керівництвом, відповідальність і вміння працювати в умовах стресу.

Практика є основою для написання магістерської кваліфікаційної роботи. Студенти збирають і систематизують інформацію, проводять експерименти,

аналізують дані, що стають емпіричною базою їхнього дослідження. При цьому є можливість дослідити методи захисту інформації на конкретному підприємстві, провести їх порівняльний аналіз, виявити недоліки та запропонувати шляхи їх усунення. Це дозволяє зробити роботу не просто теоретичною, а прикладною та науково обґрунтованою.

Методичні вказівки з проходження науково-дослідницької практики за **освітньо-науковою програмою** “Кібербезпека” розроблено для надання магістрам комплексної інформації щодо організації, змісту, завдань та порядку проведення науково-дослідницької практики. Вони покликані забезпечити систематичний підхід до виконання науково-дослідницької роботи, що відповідає сучасним вимогам у сфері кібербезпеки.

Під час практики є можливість самостійно ставити дослідницькі завдання, шукати шляхи їх вирішення, а також пропонувати інноваційні підходи до розв'язання проблем кібербезпеки. Це сприяє розвитку критичного мислення та здатності до постійного самовдосконалення, що є вкрай важливим у сфері, яка динамічно змінюється.

1 МЕТА І ЗАВДАННЯ НАУКОВО-ДОСЛІДНИЦЬКОЇ ПРАКТИКИ

Метою науково-дослідницької практики є закріплення, поглиблення та систематизація знань, отриманих під час навчання, що дає змогу здобувачам набути практичного досвіду у розв'язанні реальних завдань у сфері кібербезпеки, освоїти сучасні методи та інструменти для захисту інформаційних систем, даних і мереж, сформувати навички аналізу ризиків, розроблення та впровадження політик безпеки, зібрати, обробити та проаналізувати матеріали, необхідні для написання магістерської кваліфікаційної роботи та розвинути професійні компетенції, включаючи критичне мислення, вміння працювати в команді та самостійно приймати рішення в умовах, що постійно змінюються.

Завдання науково-дослідницької практики

Протягом практики здобувачі повинні виконати низку завдань, що безпосередньо пов'язані з темою їхньої магістерської кваліфікаційної роботи та специфікою підприємства-бази практики, а саме:

1) ознайомитись з організаційною структурою та системами безпеки підприємства;

2) провести аналіз поточних загроз і вразливостей;

3) взяти участь у розробленні або вдосконаленні заходів кіберзахисту;

4) виконати експериментальні дослідження, пов'язані з темою магістерської кваліфікаційної роботи;

5) оформити звітні документи: щоденник практики, звіт та підготувати доповід із супроводжуючою презентацією.

Виконання цих завдань дозволить здобувачам забезпечить успішне проходження практики та якісну підготовку магістерської кваліфікаційної роботи, а також забезпечити систематичний підхід до виконання науково-дослідницької роботи, що відповідає сучасним вимогам у сфері кібербезпеки.

2 КОМПЕТЕНТНОСТІ СТУДЕНТІВ ЗА МАГІСТЕРСЬКОЮ ОСВІТНЬОЮ ПРОГРАМОЮ

Унаслідок проходження науково-дослідницької практики студенти за освітньо-науковою програмою **“Кібербезпека”** повинні **знати:**

– потенційні загрози, методи оцінювання вразливостей систем і розроблення стратегії мінімізації ризиків;

– основні загрози інформаційній безпеці та методи їх нейтралізації;

– нормативно-правову базу України та міжнародні стандарти у сфері інформаційної безпеки;

– методи та інструменти оцінки ризиків інформаційної безпеки;

вміти:

– здійснювати перевірку безпеки інформаційних систем,

– виявляти слабкі місця (вразливості) та надавати рекомендації щодо їх усунення;

– працювати з різними засобами захисту інформації: антивірусним ПЗ, міжмережевими екранами, системами виявлення вторгнень (IDS/IPS), криптографічними протоколами;

– аналізувати існуючі проблеми, проводити наукові дослідження, впроваджувати новітні підходи та технології для вирішення завдань у сфері кібербезпеки;

– аналізувати складні ситуації, виявляти причинно-наслідкові зв'язки, оцінювати ризики та приймати обґрунтовані рішення в умовах невизначеності;

– ефективно спілкуватися з колегами, керівництвом та представниками інших професійних груп, а також працювати над спільними проєктами;

здобути навички:

– розроблення архітектури захищених інформаційних систем, мереж та програмного забезпечення;

– створення комплексних документів, які регламентують правила і процедури забезпечення інформаційної безпеки в організації;

– моделювання загроз, розробки архітектури безпечних систем та аналізу великих масивів даних.

3 ЗМІСТ І СТРУКТУРА НАУКОВО-ДОСЛІДНИЦЬКОЇ ПРАКТИКИ

Зміст науково-дослідницької практики визначається її керівником на основі силабуса з науково-дослідницької практики, теми магістерської кваліфікаційної роботи і відображається в індивідуальному плані студента.

Студент під час проходження науково-дослідницької практики зобов'язаний:

- ознайомитись із підприємством, його організаційною структурою, підрозділом кібербезпеки, внутрішніми положеннями та політиками;
- зібрати і систематизувати інформацію, необхідну для магістерської кваліфікаційної роботи, що включає аналіз існуючих систем захисту, виявлення вразливостей, дослідження сучасних загроз і методів протидії;
- безпосередньо прийняти участь у вирішенні реальних завдань, до яких може бути віднесено розробку політик безпеки, налаштування та адміністрування засобів захисту, проведення пентестів, розслідування інцидентів, розробку програмних модулів для підвищення безпеки;
- провести експерименти або моделювання для підтвердження гіпотез магістерської кваліфікаційної роботи;
- систематизувати отримані результати;
- вести щоденник науково-дослідницької практик за етапами їх проходження;
- скласти детальний звіт та подати його на кафедру;
- захистити основні положення, відображені у звіті.

У процесі науково-дослідницької практики студенти повинні виконати наступні завдання:

1) ознайомитися з функціями відділу інформаційної безпеки, його місцем у структурі підприємства та взаємодією з іншими підрозділами;

2) оцінити існуючі внутрішні документи, що регулюють питання захисту інформації (політики доступу, політики резервного копіювання, правила використання електронної пошти тощо);

3) вивчити законодавчі та нормативні акти України та міжнародних стандартів, що стосуються кібербезпеки та захисту персональних даних;

4) провести оцінку стану захищеності мережевої інфраструктури, веб-додатків або інших елементів інформаційної системи;

5) зібрати і систематизувати практичной матеріал, який буде використаний у магістерській кваліфікаційній роботі;

6) перевірити гіпотезу, сформульовані у магістерській кваліфікаційній роботі, на реальних даних або в умовах, близьких до реальних;

7) розробити практичні рекомендації на основі аналізу та проведених досліджень щодо вдосконалення системи інформаційної безпеки організації;

8) написати наукову частини звіту з обґрунтуванням актуальності та новизни наукової теми на основі реальних даних, отриманих під час практики.

4 ОРГАНІЗАЦІЯ ТА ТЕРМІНИ ПРОВЕДЕННЯ НАУКОВО-ДОСЛІДНИЦЬКОЇ ПРАКТИКИ

Науково-дослідницька практика проводиться у державних установах (міністерства, відомства, правоохоронні органи, Національний банк України), приватних компаніях (IT-компанії, аудиторські фірми, банки, фінансові установи, провайдери телекомунікаційних послуг), спеціалізованих відділах **(**відділи інформаційної безпеки великих підприємств, науково-дослідні інститути).

Організація науково-дослідницької 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. Науково-дослідницька практика проводиться

відповідно до індивідуальної програми науково-дослідницької практики, узгодженою студентом та науковим керівником на основі загальних підходів до її змісту та структури.

Перед початком науково-дослідницької практики проводяться консультаційні збори, на яких надається вся необхідна інформація з порядку проведення практики та консультація завідувача випускаючої кафедри 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 (Додаток А). Календарний графік студенти завіряють підписом керівника від університету та підписом керівника бази практики. За необхідності студентам на базу практики надається направлення від університету (Додаток Б).

На першому тижні науково-дослідницької практики студент повинен:

– отримати завдання для проходження науково-дослідницької практики;

– узгодити графік консультацій зі своїм керівником на кафедрі та ознайомитися з графіком відвідувань даної бази практики уповноваженими викладачами-консультантами;

– завірити підписом календарний графік у завідувача кафедри кібербезпеки або уповноваженою ним особою (для тих, хто проходить науково-дослідницьку практику на кафедрі), або у керівника іншої бази практики (для тих, хто проходить науково-дослідницьку практику за межами університету);

– завірити підписом та печаткою керівництва бази практики прибуття студента на науково-дослідницьку практику;

– пройти інструктаж із техніки безпеки на базі практики.

На останньому тижні науково-дослідницької практики студент повинен:

1) після закінчення терміну проходження науково-дослідницької практики за результатами виконаних робіт оформити робочі записи у

щоденнику та отримати відгуки керівника від кафедри (Додаток В) та керівника від бази практики (Додаток Г);

2) завірити підписом та печаткою керівництва бази практики вибуття студента з науково-дослідницької практики;

3) сформувати звіт, титульний аркуш якого підписати з боку студента, керівника від університету та керівника від бази практики; якщо базою науково-дослідницької практики не є університет, то на підпис керівника від бази практики поставити печатку підприємства (організації, установи) (Додаток Д).

Індивідуальний план науково-дослідницької практики студента повинен бути узгоджений із планом роботи організації, що є базою практики. У період науково-дослідницької практики студенти підкоряються всім правилам внутрішнього розпорядку і техніки безпеки, встановленим у підрозділі і на робочих місцях.

Після закінчення переддипломної практики студенти оформляють всю необхідну документацію відповідно до вимог відповідної програми переддипломної / науково-дослідницької практики (табл. 5).

Таблиця 5 – Програма науково-дослідницької практики за освітньо-науковою програмою “Кібербезпека” з розподілом за днями

№ п/п	Зміст роботи	Кількість днів
1	2	3
1	Проходження інструктажу з техніки безпеки	на початку практики
2	Вивчення організаційної структури, місії, завдань та основних напрямків діяльності	1 тиждень
3	Аналіз чинних політик, стандартів, засобів та інструментів захисту інформації, що використовуються на підприємстві	1 тиждень
4	Уточнення індивідуального завдання, обговорення його з керівниками від університету та підприємства	2 тиждень
5	Проведення аудитів безпеки, сканування мереж і систем на наявність вразливостей, розробка рекомендацій щодо їх усунення	3 тиждень
6	Моніторинг нових видів кібератак, аналіз інцидентів кібербезпеки, розслідування кіберзлочинів	4 тижня

7	Тестування ефективності криптографічних алгоритмів, розробка протоколів захищеної передачі даних	5 тижня

Закінчення табл. 5

1	2	3
8	Аналіз відповідності системи безпеки міжнародним стандартам (ISO/IEC 27001) та законодавчим вимогам	6 тижня
9	Збір даних, статистики, результатів експериментів для подальшого аналізу в магістерській роботі	7 тижня
10	Структуризація отриманого досвіду, висновків та результатів	7 тижня
11	Формування звіту	протягом практики

Робочий час практиканта 81 год/тиждень

Самостійна робота 570 год

5 КЕРІВНИЦТВО ТА КОНТРОЛЬ ПРОХОДЖЕННЯ НАУКОВО-ДОСЛІДНИЦЬКОЇ ПРАКТИКИ

Загальне методичне керівництво науково-дослідницькою практикою здійснюється випускаючим структурним підрозділом – кафедрою “Кібербезпека”. Загальне керівництво науково-дослідницькою практикою здійснює науковий керівник від кафедри. Для проходження науково-дослідницької практики для всіх студентів визначаються куратори від бази практики, під керівництвом яких студенти виконують поставлені в програмі завдання. Керівник практики від кафедри надає студенту організаційне сприяння та методичну допомогу у вирішенні завдань.

Керівник науково-дослідницької практики від кафедри:

- погоджує програму науково-дослідницької практики і тему завдання з науковим керівником;
- надає консультації студентам за попередньо узгодженим графіком та проводить перевірку проходження науково-дослідницької практики студентами та надає їм консультації на тих базах науково-дослідницької практики, які зазначені в графіку виїзду;
- встановлює зв'язок із керівниками науково-дослідницької практики від організації і спільно з ними складає робочу програму проведення науково-дослідницької практики;

- розробляє завдання згідно з темою магістерської кваліфікаційної роботи;
- сприяє формуванню загальної схеми виконання завдання, графіка проведення науково-дослідницької практики, режиму роботи студентів і здійснює систематичний контроль ходу практики і роботою студентів;
- бере участь у розподілі студентів за робочими місцями або переміщення їх за видами робіт;
- несе відповідальність разом із керівником науково-дослідницької практики від організації за дотримання студентами правил техніки безпеки;
- здійснює контроль дотримання термінів науково-дослідницької практики та її змісту;
- надає методичну допомогу студентам під час виконання ними індивідуальних завдань і збору матеріалів для магістерської кваліфікаційної роботи;
- оцінює результати виконання студентами програми науково-дослідницької практики та вносить їх як у вигляді оцінки, так і у вигляді відгуку за результатами роботи студента (Додаток В).

Керівник практики від бази практики:

- погоджує програму науково-дослідницької практики згідно зі встановленою темою магістерської кваліфікаційної роботи;
- надає консультації студентам щодо організації збору необхідної інформації за темою завдання;
- установлює зв'язок із керівниками науково-дослідницької практики від університету;
- розробляє тематику індивідуальних завдань;
- сприяє виконанню режиму роботи студентів і здійснює систематичний контроль проведення науково-дослідницької практики і роботи студентів;
- бере участь у розподілі студентів за робочими місцями або переміщення їх за видами робіт;

- несе відповідальність разом із керівником науково-дослідницької практики від університету за дотриманням студентами правил техніки безпеки;
- здійснює контроль дотримання термінів науково-дослідницької практики та її змісту;
- оцінює результати виконання студентами програми науково-дослідницької практики та вносить їх як у вигляді оцінки, так і у вигляді відгуку за результатами роботи студента у щоденник з науково-дослідницької практики (додаток Г).

Науковий керівник студента:

- координує постановку завдань із самостійної роботи студентів у період науково-дослідницької практики за виданим індивідуальним завданням зі збору необхідних матеріалів, надає відповідну консультаційну допомогу;
- дає рекомендації щодо вивчення спеціальної літератури;
- бере участь у роботі конференції з ведення підсумків науково-дослідницької практики.

Студент під час проходження науково-дослідницької практики отримує від керівника науково-дослідницької практики, а також від свого наукового керівника вказівки, рекомендації та роз'яснення з усіх питань, пов'язаних з організацією та проходженням науково-дослідницької практики, звітує про виконання робіт відповідно до графіка проведення науково-дослідницької практики.

Студент:

- проводить збір матеріалів за обраним завданням відповідно до графіка науково-дослідницької практики та режимом роботи підрозділу – місця проходження науково-дослідницької практики;
- отримує від керівника науково-дослідницької практики вказівки, рекомендації та роз'яснення з усіх питань, пов'язаних з організацією та проходженням науково-дослідницької практики;
- звітує про виконану роботу відповідно до встановленого графіка.

6 ЗВІТНІСТЬ ЗА РЕЗУЛЬТАТАМИ НАУКОВО-ДОСЛІДНИЦЬКОЇ ПРАКТИКИ, ЇЇ ЗАХИСТ І ПІДСУМКОВИЙ КОНТРОЛЬ

За підсумками практики студент надає на кафедру:

- щоденник практики студента;
- розгорнутий звіт про результати практики, який складається з титульного аркуша, завдання на практику, змісту, вступу, основної частини у встановленій формі, висновків (самостійної оцінки роботи), списку використаної літератури, додатків;
- презентацію та текст підготовленої доповіді за матеріалами практики.

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

Захист звітів із практики здійснюється або на конференції, присвяченій підсумкам науково-дослідницької практики в дні, встановлені керівником від кафедри.

За підсумками захисту студенту виставляється диференційований залік згідно зі встановленою університетом шкалою оцінювання.

Оцінку за науково-дослідницьку практику заносять в екзаменаційну відомість, прирівнюється до оцінок (заліків) із теоретичного навчання і враховується під час підведення підсумків загальної успішності студентів.

Атестація практики здійснюють за 100-бальною шкалою. Рівень оцінки відповідає рівню виконаної роботи і поданих матеріалів у частині опрацьованої літератури, зібраних і оброблених матеріалів, їх відповідності темі магістерської кваліфікаційної роботи.

Оцінка “відмінно” (90 – 100 балів) виставляється за умови повного виконання вимог з практики в становлений термін, готовності для включення поданих матеріалів у магістерську кваліфікаційну роботу.

Оцінка “добре” (74 – 89 балів) виставляється в разі наявності окремих недоробок, неповноти поданих матеріалів.

Оцінка “задовільно” (60 – 73 балів) виставляється в разі некомплектного і неякісного подання матеріалів, слабкої готовності для включення в магістерську кваліфікаційну роботу.

Після закінчення практики студенти складають письмові звіти і здають їх разом із щоденником практики на кафедру.

Рекомендується складати звіт про практику за структурою, наведеною в табл. 6.

Таблиця 6 – Структура звіту з науково-дослідницької практики

Розділ	Кількість сторінок
1	2
Титульний аркуш	1
Завдання на практику	1
Зміст	1
Вступ	1
1 Загальна характеристика об'єкта практики та його інформаційної інфраструктури	6
1.1 Короткий опис організації, її основної діяльності та структури	2
1.2. Загальна характеристика її інформаційної системи або мережі	2
1.3 Опис стану інформаційної безпеки, що існує в організації, та перелік основних загроз, з якими вона стикається	2
2 Аналітична частина та обґрунтування наукового дослідження	12
2.1 Проведення аналізу існуючих рішень або методик, що використовуються в організації (у контексті теми)	6
2.2. Обґрунтування актуальності та новизни щодо майбутнього дослідження, визначити яка саме проблема потребує наукового вирішення.	6
3 Опис виконаних науково-дослідних робіт	11
3.1 Опис методики, яку використовували для збору даних (“проведення глибинних інтерв'ю", “збір і аналіз мережевого трафіку", “розробка експериментальної моделі")	2

Закінчення табл. 6

1	2
3.2 Опис експерименту, який було проведено .(які дані збирали, яке програмне забезпечення використовували, які гіпотези перевіряли)	4
3.3 Проміжні результати дослідження (статистичні дані про інциденти безпеки, результати аналізу вразливостей, порівняльна таблиця ефективності різних алгоритмів, опис розробленого прототипу або моделі)	5
Висновки (як отримані результати будуть використані в магістерській кваліфікаційній роботі)	2
Список літератури	3
Додатки	

Рекомендації щодо оформлення звіту:

– **обсяг:** дотримуватися рекомендованого кафедрою обсягу звіту (зазвичай 20-40 сторінок без додатків);

– **оформлення:** дотримуватися вимог ДСТУ та методичних вказівок кафедри щодо оформлення звітів;

– **мова:** звіт пишеться державною мовою;

– **конфіденційність:** особливу увагу приділити питанням конфіденційності інформації, отриманої на базі практики. Не розголошувати комерційну таємницю, персональні дані, критичні вразливості без дозволу. Усі приклади та дані мають бути узагальненими або знеособленими;

Для студентів спеціальності **125 (F5) “Кібербезпека та захист інформації” (освітньо-наукова програма “Кібербезпека”)**

У **ВСТУПІ** необхідно вказати:

– мету та завдання практики (вказати, що повинно бути досягнуто, основну мету – це збір та аналіз наукових матеріалів для магістерської кваліфікаційної роботи, а також проведення первинних досліджень);

– терміни та місце проходження практики (вказати точні дати та назву організації);

– зв'язок з темою магістерської кваліфікаційної роботи (пояснити, як обране місце практики та виконані завдання корелюють із темою магістерської кваліфікаційної роботи).

У **ПЕРШОМУ РОЗДІЛІ** необхідно надати короткий опис організації, її основної діяльності та структури; загальну характеристику її інформаційної системи або мережі, якщо це дозволено; опис стану інформаційної безпеки, що існує в організації, та перелік основних загроз, з якими вона стикається.

У **ДРУГОМУ РОЗДІЛІ** необхідно провести аналіз існуючих рішень або методик, що використовуються в організації, у контексті теми; на основі цього аналізу обґрунтувати актуальність та новизну майбутнього дослідження; визначити, яка саме проблема потребує наукового вирішення.

У ТРЕТЬОМУ РОЗДІЛІ описати методику, яку було використано для збору даних (“проведення глибинних інтерв'ю”, “збір і аналіз мережевого трафіку”, “розробка експериментальної моделі”); представити опис експерименту, який було проведено (які дані було зібрано, яке програмне забезпечення використовувалось, які гіпотези перевірялись); навести проміжні результати дослідження (статистичні дані про інциденти безпеки, результати аналізу вразливостей, порівняльна таблиця ефективності різних алгоритмів, опис розробленого прототипу або моделі); пояснити, як отримані дані та висновки будуть використані в магістерській кваліфікаційній роботі.

У **ВИСНОВКАХ** необхідно підсумувати результати проходження практики; зробити остаточні висновки щодо підтвердження або спростування ваших попередніх гіпотез; сформулювати, який науковий доробок отримано під час практики і як це вплине на фінальну частину вашої магістерської кваліфікаційної роботи; оцінити свій особистий внесок у наукове дослідження.

Зміст звіту з практики визначається особистим завданням, що видано студенту під час від'їзду до бази практики.

Перший аркуш звіту з практики є титульним. Зразок його оформлення наведено в додатку Д.

Другий аркуш має назву “Завдання на практику” і повинен містити

перелік завдань, які повинні бути вирішені в ході проходження практики. Цей аркуш повинен бути підписаний студентом, який має виконати ці завдання, та викладачем-керівником (див. додаток Е).

Увесь текст звіту з практики повинен бути оформлений згідно з додатком Ж.

У рекомендованій літературі (див. додаток Ж) повинно бути вказано не тільки перелічені ДСТУ, які було використано під час виконання завдань практики та оформлення бібліографічного опису, але й джерела, в яких розкриваються питання предметної області, що аналізується за обраною тематикою завдання.

Список використаної літератури необхідно оформити згідно з рекомендаціями, наведеними у додатку Ж.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бєлов М. О., Іщенко В. В. Інформаційна безпека: основи теорії та практики. Київ : Видавничий дім “Слово”, 2023. 412 с.
2. Бубенко А. Р. Системи управління інформаційною безпекою. Київ : Освіта України, 2021. 300 с.
3. Гаврилов О. М., Сухомлин В. О. Кібербезпека: основи та принципи захисту : навч. посіб. Київ : Видавнича група BHV, 2021. 320 с.
4. Григор’єв А. М., Петренко В. В. Системи менеджменту інформаційної безпеки: навч. посіб. Київ: Центр учбової літератури, 2020. 352 с.
5. Дейвіс Р., Куценко О. Управління ризиками інформаційної безпеки: монографія. Харків: Фактор, 2021. 280 с.
6. Довгань О., Ткачук Т. Кіберризики критичної інфраструктури: від аналізу загроз до впровадження рішень [Текст] : наук.- практ. посіб.; Держ. наук. установа “Ін-т інформації, безпеки і права Нац. акад. прав. наук України”. Київ ; Одеса : Фенікс, 2024. 70 с.
7. Додонов О. Г., Додонов О. О., Ільясов М. С. Кібербезпека та кіберзахист : навч. посіб. Київ : НАУ, 2022. 380 с.
8. Дорошенко А. Захист персональних даних у сфері Data Science: імплементація GDPR в Україні [Текст] : [монографія] ; “Erasmus+” Programme of the European Union ; [Нац. ун-т “Львів. політехніка”]. Львів : Вид-во Тараса Сороки, 2022. С. 80-88.
9. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи та засоби убезпечення. Системи управління інформаційною безпекою. Вимоги. Київ : Держстандарт України, 2015. 48 с.
10. Загальний регламент про захист даних (GDPR) : Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (дата звернення: 13.07.2025).

11. Закон України “Про основні засади забезпечення кібербезпеки України” від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. С. 138–150.

12. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”: [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 18.08.2025).

13. Зубенко С. В., Ракша О. В. Мережева безпека : навч. посіб. Київ: ІТНВУ, 2019. 256 с.

14. Ігнатенко Р. С. Захист вебдодатків від DDoS-атак: сучасні підходи. Наукові праці Інституту кібербезпеки. 2023. Вип. 1 (45). С. 112-120.

15. Кіберзахист в умовах гібридної війни: монографія. / за заг. ред. О. В. Довгаля. Харків : ТОВ “Видавництво “Нове слово”, 2021. 288 с.

16. Когут О. В. Міжнародна кібербезпека: виклики та співпраця : навч. посіб. Львів : ЛНУ ім. І. Франка, 2021. 250 с.

17. Козаченко Ю. М., Мельник О. М. Застосування машинного навчання для виявлення аномалій у мережевому трафіку. Вісник кібербезпеки. 2023. № 2. С. 45–56.

18. Кривогуз І. М. Криптографічні методи захисту інформації. Львів : Видавництво Львівської політехніки, 2019. 250 с.

19. Ліщук В. В. Аналіз сучасних кіберзагроз в умовах гібридної війни. Інформаційна безпека. 2024. Т. 1, № 1. С. 110–125.

20. Павленко О. В. Аналіз сучасних методів кіберрозвідки та протидія цілеспрямованим атакам. Проблеми кібербезпеки. 2024. № 1 (25). С. 45-53.

21. Потапова В. Г., Євсеєв С. П. Реагування на кіберінциденти : навч. посіб. Київ: НАУ, 2020. 192 с.

22. Потопальський В. В., Лисенко О. А., Семенов І. Г. Захист інформації: криптографічні методи. Київ : Центр навчальної літератури, 2022. 356 с.

23. Скляров В. А. Безпека програмного забезпечення та даних : навч. посіб. Харків : Ранок, 2023. 360 с.

24. Ткач Ю. М. Методи та моделі побудови захищеного кіберпростору [Текст] : автореф. дис. ... канд. техн. наук : 21.05.01 /; Нац. авіац. ун-т. Київ, 2021. 20 с. : рис., табл.

25. Щеголенкова Н. М. Аудит інформаційної безпеки: навч. посіб. Львів: Магнолія Плюс, 2022. 280 с.

26. Щербина Ю. А. Криптографія. Захист інформації в комп'ютерних системах : навч. посіб. Львів : Магнолія Плюс, 2018. 416 с.

27. CERT-UA. Річний звіт про кіберінциденти у 2023 році. Державний центр кіберзахисту CERT-UA. 2024. URL: https://cert.gov.ua/article/11223 (дата звернення: 17.08.2025).

28. CERT-UA. Звіт про кіберінциденти та кібератаки на об'єкти критичної інфраструктури України. Державний центр кіберзахисту CERT-UA. 2024. URL: https://cert.gov.ua/reports (дата звернення: 18.08.2025).

29. ENISA Threat Landscape Report 2023. European Union Agency for Cybersecurity (ENISA). 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 18.08.2025).

30. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. URL: https://www.iso.org/standard/82875.html (access on: 18.08.2025).

31. Kaspersky Security Bulletin. Statistics 2024. Kaspersky. 2024. URL: https://www.kaspersky.com/about/security-bulletin (access on: 18.08.2025).

32. Microsoft. Digital Defense Report 2024. URL: https://www.microsoft.com/en-us/security/business/reports/digital-defense-report-2024 (acces on: 17.08.2025).

33. Modeling of security systems for critical infrastructure facilities [Text] : monograph / [R. Korolev et al.] ; ed. by Serhii Yevseiev [et al.]. Kharkiv : PC Technology Center, 2022. XIV, P. 169-181.

34. NIST Cybersecurity Framework (National Institute of Standards and Technology Cybersecurity Framework). URL: https://www.nist.gov/cyberframework (acces on: 13.07.2025).

35. Simpson Michael T., Antill Nicholas, Backman Kent. Hands-On Ethical Hacking and Network Defense. Boston: Cengage Learning, 2022. 720 p.

ДОДАТКИ

ДОДАТОК А

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

Форма № ВП-03

ЩОДЕННИК ПРАКТИКИ

Науково-дослідна
(вид і назва практики)

студента
(прізвище, ім’я, по-батькові)

Інститут/факультет комп'ютерних наук та інформаційних технологій

кафедра кібербезпеки

Рівень вищої освіти магістр

Спеціальність 125 (F5) Кібербезпека та захист інформації
(назва)

Освітня програма Кібербезпека
(назва)

Курс 2 рік навчання Група КН-

Продовження дод. А

Студент_____

(прізвище, ім’я, по-батькові)

Прибув на підприємство

“____”_____ 20__ р. _____

(підпис, завірений печаткою)

_____

(посада, прізвище та ініціали відповідальної особи)

Вибув з підприємства

“____”_____ 20 __ р. _____

(підпис, завірений печаткою)

_____

(посада, прізвище та ініціали відповідальної особи)

Закінчення дод. А

Календарний графік проходження практики

(освітньо-наукова програма “Кібербезпека”)

Назви робіт	Місце виконання робіт	Термін виконання тиждень (доба)	Відмітки про виконання
Проходження інструктажу з техніки безпеки		на початку практики	
Вивчення організаційної структури, місії, завдань та основних напрямків діяльності		1 тиждень	
Аналіз чинних політик, стандартів, засобів та інструментів захисту інформації, що використовуються на підприємстві		1 тиждень	
Уточнення індивідуального завдання, обговорення його з керівниками від університету та підприємства		2 тиждень	
Проведення аудитів безпеки, сканування мереж і систем на наявність вразливостей, розробка рекомендацій щодо їх усунення		3 тиждень	
Моніторинг нових видів кібератак, аналіз інцидентів кібербезпеки, розслідування кіберзлочинів		4 тижня	
Тестування ефективності криптографічних алгоритмів, розробка протоколів захищеної передачі даних		5 тижня	
Аналіз відповідності системи безпеки міжнародним стандартам (ISO/IEC 27001) та законодавчим вимогам		6 тижня	
Збір даних, статистики, результатів експериментів для подальшого аналізу в магістерській роботі		7 тижня	
Структуризація отриманого досвіду, висновків та результатів		7 тижня	
Формування звіту		протягом практики	

Керівники практики:
від Університету _____ (підпис) _____ (прізвище та ініціали)

Від підприємства,
організації, установи _____ (підпис) _____ (прізвище та ініціали)

ДОДАТОК Б

Форма № ВП-02

КЕРІВНИКУ

_____

_____

_____

НАПРАВЛЕННЯ НА ПРАКТИКУ

(є підставою для зарахування на практику)

Згідно з договором від "_____"_____ 20___ р. № _____, який укладено з

_____,

повне найменування підриємства, організації, установи

направляємо на практику студентів ___ курсу, які навчаються за спеціальністю Кібербезпека та захист інформації освітньою програмою Кібербезпека.

Назва практики магістерська

Строки практики з _____ по _____ 20 р.

Керівник практики від кафедри Кібербезпеки та захисту інформації

назва кафедри

_____,

посада, прізвище, ім'я, по батькові

ПРІЗВИЩА, ІМЕНА ТА ПО БАТЬКОВІ СТУДЕНТІВ	ДОДАТКОВА ІНФОРМАЦІЯ

М.П. Керівник

Практики НТУ "ХПІ" _____

(підпис) (прізвище та ініціали)

Примітки:

1. Форма служить підставою для прийому студентів на практику підприємством, установою, організацією.
2. Формат бланка – А5 (148×210 мм), 2 сторінки.

ДОДАТОК В

Відгук керівника від університету про проходження практики

У відгуку керівника практики від університету обов'язково повинно бути зазначено таке:

- вказується відповідність виконання поставлених завдань встановленим строкам календарного графіка;
- наголошується на ступені повноти вирішення питань, які розглядаються в роботі;
- звертається увага на обсяг і якість виконаної студентом роботи,
- звертається увага на своєчасність і правильність ведення щоденника практики;
- зазначається обов'язковість відвідування консультацій, які проводив керівник;
- ураховуються відгуки спеціалістів із бази практики, які надаються керівнику під час відвідування бази практики.

ДОДАТОК Г

Відгук куратора практики від підприємства

У відгуку керівника практики від підприємства повинно бути зазначено таке:

- повнота виконання студентом програми проходження практики;
- якість написання студентом звіту про проходження практики, його відповідність установленим вимогам, реаліям бази практики;
- рівень підготовленості практиканта до професійної діяльності за теоретичними знаннями і практичними навичками;
- відношення студента до роботи, його організованість і дисциплінованість;
- практична значимість пропозицій практиканта, викладених у звіті, щодо поліпшення певних аспектів завдань, що вирішуються тощо;
- вміння працювати в колективі, рівень комунікабельності, громадську позицію та інші особисті риси, що проявились під час практики.

ДОДАТОК Д

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУ КОМП'ЮТЕРНИХ НАУКТ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КІБЕРБЕЗПЕКИ

Звіт

з науково-дослідної практики

на тему: “ …”

Виконав(ла): студент(ка) 2р.н., групи <шифр>, спеціальності 125 (F5) “Кібербезпека та захист інформації”
П. І. Б. студента(ки)

Керівник від
бази практики _____ _____
(підпис, печатка) (науковий ступінь, посада, П. І. Б.)

Керівник від ЗВО _____ _____
(підпис) (науковий ступінь, посада, П. І. Б.)

Харків – 20___ рік

ДОДАТОК Е

ЗАВДАННЯ НА ПРАКТИКУ

1. Назва завдання: _____
_____
_____
2. Строк подання звіту _____
3. Вхідні дані до завдання: ДСТУ з оброблення інформації, літературні джерела, технічна документація <назва об’єкта>, матеріали практики.
4. Перелік графічного матеріалу: _____
_____
_____

Керівник від ЗВО _____
(підпис) (посада, П. І. Б.)

Студент/ка _____
(підпис) (П. І. Б.)

ДОДАТОК Ж

Правила оформлення звіту

Інтервал	Звіт формують на одному боці аркуша білого паперу формату А4 (210х297 мм) через 1,5 міжрядкового інтервалу; зверху, знизу – 0 пт
Шрифт	Times New Romal, кегель – мітел (14 типографських пунктів).
Абзацний відступ	1,25 см
Відступи	Ліворуч, праворуч – 0 см
Поля	Текст звіту необхідно формувати, залишаючи поля таких розмірів: ліве – 25 мм, праве – 10 мм, верхнє – 20 мм, нижнє – 20 мм
Розділи	Вступ, Висновки, Зміст, Список літератури, Назва розділу – великими літерами, посередині нового аркуша без абзацного відступу: **1 НОВА ЕРА** …
Підрозділи	Назва підрозділу – з першої великої літери, інші літери – маленькі, з абзацного відступу, вирівнюти з а шириною: **1.1 Опис**… Пустий рядок перед та після назви розділу.
Рисунки	Посилання на рисунок: статистикою, що представлена у звіті, щороку кількість скарг (або інцидентів) зростає, при цьому значно інтенсивніше й підвищуються збитки від успішно впроваджених загроз, ШПЗ, тощо (рис 1.1). Пустий рядок від рисунку зверху та знизу, рисунок – посередині, підпис під рисунком без пустого рядка посередині аркуша:

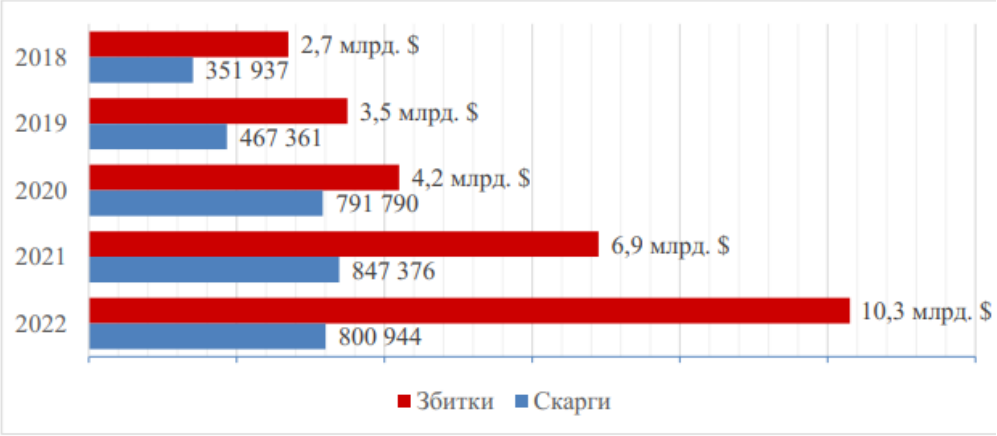
<table>
<tr><td></td><td>


Рисунок 1.1 – Скарги та збитки через кіберзагрози в 2018-2022 році
Посилання – наведено на рис. 1
</td></tr>
<tr><td>Таблиці</td><td>
Посилання на таблицю:
Використовуючи запропоновану вище процедуру отримано результуючу модель на базі НДР, описану в табл. 3.1. Побудоване НДР має значно більшу
Пустий рядок від таблиці зверху та знизу, таблиця – посередині, назва таблиці з абзацного відступу без пустого рядка за шириною аркуша:
Таблиця 3.1 – Результуюча модель на базі НДР
<table>
<tr><th>Код ознаки</th><th>Кількість нечітких множин</th><th>Використання у побудованій моделі</th><th>Код ознаки</th><th>Кількість нечітких множин</th><th>Використання у побудованій моделі</th></tr>
<tr><td>A</td><td>3</td><td>+</td><td>L</td><td>4</td><td>+</td></tr>
<tr><td>B</td><td>2</td><td>+</td><td>M</td><td>6</td><td>-</td></tr>
</table>
</td></tr>
<tr><td>Форму-ли</td><td>
Іншим прикладом є метод, що базується на показнику Херста [20, 21]
$$H = \frac{\ln\left(\frac{R}{S}\right)}{\ln(\alpha N)}, \quad (1.3)$$
де: S – середньоквадратичне відхилення часового ряду;
R – розмах накопиченого відхилення часового ряду;
N – розмір часового ряду;
α – заданий параметр, який більший від нуля.
</td></tr>
</table>

Закінчення дод. Ж

Посилання	В роботах [24, 25] досліджено модель ідентифікації шкідливого програмного забезпечення на основі контекстно-вільних граматик. Представлена В роботах [39-42] описані різні модифікації глибоких нейронних мереж для виявлення саме ШПЗ. Разом із тим, такі моделі мають велику кількість хибних
Список літератури	Оформлюється або за алфавітом (спочатку на кириліці, потім – на латиниці), або за згадованістю по тексту (Бібліографічний опис списку використаних джерел оформлено згідно з IEEE Style, що входить до Додатку 3, Наказу МОН «Про затвердження вимог до оформлення дисертації» від 12 січня 2017 року № 40) *Електронне посилання:* 1. Australian Cyber Security Centre, *Annual Cyber Threat Report, July 2021 to June 2022* [Online]. Available: https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022 [accessed Jul. 31, 2023]. *Журнал:* 19. В. В. Челак, С. Г. Семенов, та С. Ю. Гавриленко, "Розробка шаблонів ідентифікації стану комп'ютерних систем на основі BDS-тестування", *Вісник НТУ "ХПІ". Інформатика та моделювання*, № 21, с. 118-125, Харків, 2016. *Книга:* 33. G. J. McLachlan, *Discriminant Analysis and Statistical Pattern Recognition*. Wiley Interscience, 2004, 552 с.
Зміст	Формується електронними засобами

ЗМІСТ

Навчальне видання

Методичні вказівки
до проведення науково-дослідницької практики
для студентів денної форми навчання другого (магістерського) рівня вищої освіти за спеціальністю 125 (F5) “Кібербезпека та захист інформації”

Укладачі:
КОРОЛЬ Ольга Григорівна
МІЛЕВСЬКИЙ Станіслав Валерійович
ГАВРИЛОВА Алла Андріївна

Відповідальний за випуск проф. Євсеєв С. П.
Роботу рекомендував до друку проф. Євсеєв С. П.

В авторській редакції

План 2025 р., поз. 791

Підп. до друку .Гарнітура Times New Roman.
Видавничий центр НТУ “ХПІ”.
вул. Кирпичова, 2, м. Харків, 61002
Свідоцтво про державну реєстрацію ДК № 5478 від 21.08.2017 р.
Електронне видання