КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

Безпека інформаційних систем та мереж

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
до виконання курсових робіт

освітній ступінь **бакалавр**

галузь знань **12 Інформаційні технології**

Спеціальність **125 Кібербезпека**

спеціалізація **Безпека інформаційних і комунікаційних систем в економіці**

Київ 2021

Автори: В.І. ПАШОРІН, кандидат технічних наук, професор
кафедри інженерії програмного забезпечення та кібербезпеки
Ю.В. КОСТЮК, асистент кафедри інженерії програмного
забезпечення та кібербезпеки
Ю.О. САМОЙЛЕНКО, кандидат технічних наук, доцент
кафедри інженерії програмного забезпечення та кібербезпеки
Л.О. ВЛАСЕНКО, кандидат технічних наук, доцент
кафедри інженерії програмного забезпечення та кібербезпеки
Т.В. САВЧЕНКО, кандидат технічних наук, доцент
кафедри інженерії програмного забезпечення та кібербезпеки

Обговорено та схвалено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки 14 вересня 2021 р., протокол № 3 .

Рецензент: Н.О. Котенко, кан. пед. наук, доцент кафедри інженерії
програмного забезпечення та кібербезпеки

Безпека інформаційних систем та мереж

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
до виконання курсових робіт

освітній ступінь	**бакалавр**
галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
спеціалізація	**Безпека інформаційних і комунікаційних систем в економіці**

ЗМІСТ

ВСТУП

Виконання і захист курсової роботи є однією з найважливіших форм навчальної роботи. Вона має на меті прищепити навички самостійної роботи, виявити знання студентів по даній дисципліні та уміння застосовувати ці знання в практичній роботі по обраній ними спеціальності.

Курсова робота – є навчально-дослідницькою роботою, яка дає змогу виявити рівень засвоєння ним теоретичних знань та практичної підготовки, здатність до самостійної роботи за обраною спеціалізацією. Методичні рекомендації встановлюють вимоги щодо структури, змісту, оформлення та тематики курсових робіт, призначені здобувачам вищої освіти бакалаврської програми за фахом, а також для керівників з курсових робіт.

У процесі виконання курсової роботи студент повинен самостійно працювати з навчальною і науково-технічною літературою, уміти узагальнювати отримані знання, робити обґрунтовані висновки, формулювати рекомендації з вибору технічних і програмних засобів для вирішення конкретного завдання.

Дані методичні рекомендації висувають загальні вимоги до організації та проведення курсової роботи, тематики, змісту та обсягу, порядку розробки та захисту курсових робіт (КР) у відповідності до програми дисципліни «Безпека інформаційних систем та мереж» спеціальності 125 «Кібербезпека» спеціалізації «Безпека інформаційних і комунікаційних систем в економіці» та діючих нормативно-технічних документів КНТЕУ.

Метою роботи є отримання знань і навичок аналізу загроз і заходів щодо їх запобігання програмно-апаратними засобами захисту інформації, а також вбудованими механізмами захисту загальносистемного програмного забезпечення.

Керівнику курсової роботи необхідно забезпечити оптимальні умови для плідної самостійної роботи студентів. Цій меті повинні сприяти продумана методика керівництва і консультування, допомога в пошуку методичної та технічної документації, науково-технічної літератури, а також систематичний контроль за виконанням курсової роботи.

Загальні вимоги до курсової роботи:

- чіткість побудови;
- логічна послідовність викладу матеріалу, переконлива аргументація;
- точність викладу, яка виключає можливість суб’єктивного та неоднозначного тлумачення;
- конкретність викладу результатів роботи;
- доведення висновків та обґрунтованість рекомендацій.

ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. МЕТА ТА ЗАВДАННЯ КУРСОВОЇ РОБОТИ

Відповідно до «Положення про організацію виконання та захисту курсових робіт (проектів) у КНТЕУ» та навчального плану студентів спеціальності 125 «Кібербезпека» спеціалізації «Безпека інформаційних і комунікаційних систем в економіці» освітнього ступеня «бакалавр» виконують курсову роботу (КР) з дисципліни «Безпека інформаційних систем та мереж».

Курсова робота – складовий компонент навчального процесу вивчення дисципліни. Виконання курсової роботи − перший самостійний крок майбутнього фахівця, коли право остаточного вибору інженерно-технічних рішень і відповідальність за їх прийняття цілком належить його автору.

Метою курсової роботи є:

- закріплення, поглиблення й узагальнення знань, отриманих студентами за час вивчення дисципліни «Безпека інформаційних систем та мереж» з поглибленою спеціальною підготовкою в сфері безпеки інформаційних і комунікаційних систем;
- здійснення проведення моніторингу та прогнозування комп’ютерних зловживань та аномалій;
- протидіяти несанкціонованому проникненню в інформаційні системи;
- відновлювати штатне функціонування інформаційно-телекомунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження;
- формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління кібербезпекою;
- виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту інформації та інформаційних систем;
- застосовувати криптографічні методи захисту інформаційних і комунікаційних ресурсів;
- використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
- впроваджувати та забезпечувати функціонування комплексних систем захисту;
- забезпечувати впровадження та дотримання політики безпеки.

Завдання до курсової роботи передбачає: здійснювати проведення моніторингу та прогнозування комп’ютерних зловживань та аномалій; протидіяти несанкціонованому проникненню в інформаційні системи; відновлювати штатне функціонування інформаційно-телекомунікаційних

систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження; формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління кібербезпекою; виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту інформації та інформаційних систем; застосовувати криптографічні методи захисту інформаційних і комунікаційних ресурсів; використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; впроваджувати та забезпечувати функціонування комплексних систем захисту; забезпечувати впровадження та дотримання політики безпеки; вирішувати задачі захисту інформації, що обробляється в ІТС з використанням сучасних методів та засобів криптографічного захисту інформації; визначати відомості, які відносяться до різних видів конфіденційної інформації, організовувати допуск та доступ персоналу до конфіденційної інформації згідно встановленої політики інформаційної та/або кібербезпеки; демонструвати знання та розуміння основ побудови комп'ютерних мереж та описати в загальних поняттях і термінах принципи та методи організації мережевих комунікацій; демонструвати знання та розуміння організації баз даних та розробляти проекти баз даних інформаційних систем, використовуючи сучасні методи і моделі інформаційної та кібербезпеки; продемонструвати знання та розуміння технологій проектування комп'ютерних систем захисту інформації; демонструвати знання та розуміння діагностування та експлуатації комп'ютерних систем захисту інформації та застосовувати на практиці засоби автоматичного контролю і діагностування.

Виконання курсової роботи з дисципліни «Безпека інформаційних систем та мереж» та її захист є формою контролю рівня знань студентів за вивченням даної навчальної дисципліни.

Наукове керівництво курсової роботи здійснюється викладачами кафедри інженерії програмного забезпечення та кібербезпеки. Керівник проводить індивідуальні консультації для студентів за відповідним графіком, встановленим на кафедрі.

Цілями виконання курсової роботи для студента є: формування умінь узагальнювати, систематизувати науковий текст і аналізувати вивчений матеріал; підвищення самооцінки своєї інтелектуальної праці; поглиблення і закріплення знань, отриманих в результаті вивчення спеціальної літератури та інформаційних джерел; розвиток вміння пов'язувати теоретичні положення з реальними умовами сучасної практики кібербезпеки.

Курсова робота спрямована на вивчення одного з етапів робіт по проведення аудиту безпеки ІТС, а саме на оцінку ефективності програмних і апаратних рівнів існуючої системи захисту ІТС із застосуванням спеціалізованих інструментаріїв і методів.

Метою роботи є отримання знань і навичок аналізу загроз і заходів щодо їх запобігання програмно-апаратними засобами захисту інформації, а також вбудованими механізмами захисту загальносистемного програмного забезпечення.

Виконання курсової роботи допоможе студенту глибше усвідомити вивчений матеріал, привести у відповідність теоретичні знання і практичну частину дисципліни, визначити область активного застосування результатів проведеного дослідження. Матеріал в усьому тексті роботи рекомендовано надавати в безособовій формі («можна зробити висновок ...» і т.п.), або від третьої особи, мається на увазі, що робота виконується спільно з науковим керівником - «Авторами запропоновано ...», «В роботі розглядається ...».

На виконання роботи відводиться один семестр. Студент має виконати курсову роботу згідно з графіком та вчасно подати її на кафедру.

Курсова робота повинна відповідати таким вимогам:

- бути цілеспрямованою, тобто присвяченою дослідженню однієї проблеми;
- відповідати сучасному рівню управлінської науки;
- бути логічно та послідовно структурованою за змістом;
- вирізнятися: глибиною дослідження та повнотою висвітлення визначених питань; переконливістю аргументації викладених думок; точністю і стислістю формулювань, конкретністю викладу матеріалу; обґрунтованістю висновків і рекомендацій; грамотністю оформлення пошукового апарату роботи.

В ході виконання курсової роботи, як правило, виділяються три етапи.

Перший етап - підготовчий, який визначає початкові позиції і розробку програми дослідницької діяльності і має наступні цілі:

- ознайомлення з методичними рекомендаціями щодо виконання курсової роботи;
- затвердження в ході співбесіди з керівником остаточного варіанту теми;
- складання плану курсової роботи;
- обговорення плану курсової роботи з керівником.

Другий етап – основний, включає:

- написання теоретичної частини курсової роботи;
- написання практичної частини курсової роботи.

Третій етап - підсумковий, що передбачає оформлення результатів, має наступні цілі:

- попереднє обговорення курсової роботи;
- остаточне оформлення курсової роботи;
- підготовка тексту доповіді, наочних матеріалів для захисту;
- захист курсової роботи перед комісією.

Курсова робота є самостійною роботою студента. Відповідальність за правильність аналітичних висновків, результатів розрахунків і моделювання, а також оформлення несе студент − автор КР.

1.2. ТЕМАТИКА КУРСОВОЇ РОБОТИ

Спрямування КР повинне забезпечувати творчу роботу студента та самостійне розв'язання окремих технічних завдань. Вміст та структура курсової роботи (КР) повинні враховувати специфіки напряму та вимоги освітньої програми.

Тематика КР тісно пов'язана з майбутньою спеціальністю студентів та присвячена важливому аспекту захисту інформаційних систем та мереж. Для виконання КР пропонується застосування сучасних інформаційних технологій у вигляді інструментів навантажувального тестування та моніторингу розподілених ресурсів, хмарних і мобільних технологій, технології віртуалізації та розпізнавання образів, використання методів обробки та аналізу отриманих даних. На початковому етапі виконання КР визначаються: порівняльна характеристика та особливості функціонування об'єкта дослідження, сучасні інструменти моніторингу та навантажувального тестування, математична модель процесу порушення доступності розподілених інформаційних і обчислювальних ресурсів; застосовуються статистичні методи дослідження, математичного та імітаційного моделювання.

Зміст КР визначається завданням, яке видається на консультації викладачем кожному студенту. КР охоплює декілька послідовних етапів, які, в загальному випадку, пов'язані з аналізом предметної області та змістовною постановкою задачі, розробкою індивідуального технічного завдання, вибором форми подання задачі, розробкою математичної моделі об'єкта дослідження, вибором оптимального алгоритму реалізації задачі, з розробкою сценарію навантаження на об'єкт дослідження, проведенням досліджень роботи програми та формулюванням обґрунтованих висновків щодо отриманих в роботі результатів. Кожен етап роботи обов'язково має знайти своє відображення в пояснювальній записці, що містить вхідні та вихідні дані, пояснювальні матеріали, які пов'язані з виконанням КР.

З урахуванням викладеного тематика курсового проектування повинна:

- бути актуальною і відповідати сучасному стану науки і техніки;
- відображати перспективи розвитку відповідних галузей техніки з урахуванням останніх наукових досліджень;
- стимулювати студентів на творчий пошук нових науково-технічних, проектних та інших рішень;
- викликати у студентів необхідність опрацювання спеціальної науково-технічної літератури;

– передбачати вибір сприйнятого вирішення поставленого завдання на основі використання сучасних засобів комп'ютерної техніки;
– бути націленою на вирішення задач, які є актуальними для організацій, в яких проводиться курсове проектування.

Виконання курсової роботи з однієї теми кількома студентами однієї групи не припустиме. Обрані студентами й узгоджені з науковими керівниками теми робіт затверджуються на засіданні кафедри. Курсові роботи виконанні студентами на теми, які не затверджені кафедрою не розглядаються.

Студент може запропонувати власну тему, обґрунтувавши актуальність тематики, доцільність розроблення і склавши технічне завдання, яке затверджується керівником курсової роботи.

1.3. ПРИКЛАДИ ТЕМ КУРСОВОЇ РОБОТИ

1. Розробка програмного забезпечення для пошуку шкідливих програм в ОС Windows
2. Розробка програмного забезпечення для тестування антивірусних програм в ОС Windows.
3. Розробка програмного забезпечення для перевірки захищеності ОС Windows.
4. Розробка системи захищеного резервного копіювання файлів з використанням RAID-масивів.
5. Захист інформації при використанні електронної пошти.
6. Комплексний захист інформації на приватному підприємстві.
7. Комплексний підхід до забезпечення захисту конфіденційної інформації на приватному підприємстві.
8. Організація захисту персональних даних на підприємстві.
9. Організація протидії загрозам безпеки інформації організації на підприємстві.
10. Побудова типової моделі загроз безпеки інформації на підприємстві.
11. Розробка комплексу режимних заходів щодо збереження конфіденційної інформації.
12. Розробка системи захисту комерційної інформації.
13. Розробка заходів з технічного захисту конфіденційної інформації на підприємстві.
14. Розробка політики безпеки на приватному підприємстві.
15. Розробка системи захисту інформації підприємства.
16. Захист комерційної таємниці на підприємстві.
17. Розробка комплексної системи інженерно-технічного захисту інформації на підприємстві.
18. Методи і способи протидії від витоку інформації по технічним каналам.

19. Основні положення і принципи побудови технічного захисту інформації.
20. Розробка пропозицій по вибору технічних засобів системи контролю і управління доступом для захисту інформації підприємства.
21. Розробка методики захисту персональних даних на підприємстві і її реалізація.
22. Організаційний захист об'єктів інформаційних систем.
23. Програмно-технічні засоби і способи забезпечення інформаційної безпеки.
24. Шляхи вирішення проблем захисту інформації в мережах.
25. Захист інформації в мережах і хмарних системах.
26. Безпека програмного забезпечення і мобільних додатків.
27. Розробки системи аутентифікації користувачів.
28. Безпека та захист комп’ютерних мереж та систем.
29. Сервіси безпеки та механізми її порушень.
30. Дослідження засобів захисту операційних систем.
31. Захист операційних систем і забезпечення безпеки баз даних.
32. Аналіз ризику безпеки інформаційних систем.
33. Опис стану оформлення та надання послуг електронного цифрового підпису.
34. Організаційні заходи по відновленню працездатності системи у випадку виникнення нештатних ситуацій.
35. Організаційні та технічні заходи по резервуванню критично важливої інформації.
36. Прогнозування можливих загроз і аналізу пов’язаного з ними ризику для інформаційної системи.
37. Прийняття принципових рішень в галузі безпеки на основі поточного стану інформаційної системи.
38. Введення комплексних систем захисту інформації в дію.
39. Розробка комплексної системи захисту інформації.
40. Методи моделювання автоматизованої системи захисту інформації.
41. Опис сучасних загроз для інформації при створенні комплексної системи захисту інформації.
42. Захист інформації в автоматизованих системах від витоку інформації по радіоканалу.
43. Захист інформації в автоматизованих системах від витоку інформації по каналам комунікацій.
44. Захист інформації в автоматизованих системах від витоку інформації по оптичному каналу.
45. Захист інформації в автоматизованих системах від витоку інформації по бездротовим канал зв’язку.
46. Захист інформації в автоматизованих системах від витоку інформації

по побічному електромагнітному випромінюванню.
47. Захист інформації в автоматизованих системах від витоку інформації по акустичному каналу.
48. Захист інформації в автоматизованих системах від витоку інформації по інфочервоному каналу.
49. Захист інформації при проведенні конфедіційних нарад.
50. Інженерно-технічні системи захисту інформації.
51. Програмно-апаратні системи захисту інформації.
52. Правові аспекти захисту інформації.
53. Порядок створення комплексної системи захисту інформації на підприємстві.
54. Пошук засобів негласного отримання інформації, як елемент комплексного захисту інформації.
55. Побудова інформаційної моделі системи управління захистом об’єктів.
56. Порядок проведенні експертизи комплексної системи захисту.

2. РОЗПОДІЛ ФУНКЦІОНАЛЬНИХ ОБОВ'ЯЗКІВ

2.1. КАФЕДРА

Кафедра несе повну відповідальність за хід виконання курсових робіт в освітньому процесі, в зв'язку з чим:

- розроблює відповідне Положення про виконання курсових робіт на кафедрі,
- критерії оцінок та іншу необхідну методичну документацію,
- щорічно переглядаючи їх на початку навчального року і доводячи до відома студентів через керівників на початку виконання курсових робіт;
- вирішує питання щодо організації та проведення передбаченого навчальним планом виконання курсових робіт у закріплених за ним дисциплінах;
- заздалегідь формує та затверджує тематику курсових робіт;
- регулярно заслуховує на засіданнях питання організації виконання захисту курсових робіт та подає до деканату інформацію про порушення студентами графіка виконання курсових робіт;
- формує комісії для захисту курсових робіт і організовує їх роботу;
- здає захищені проекти до архіву, де вони зберігаються у встановленому порядку;
- обговорює на засіданнях підсумки виконання курсових робіт і заходи щодо підвищення їх якості;

– розробляє і переглядає критерії оцінок курсових робіт.

2.2. Деканат

Деканат здійснює загальний контроль за організацією та ходом виконання курсових робіт на кафедрі, у зв'язку з чим:

– своєчасно інформує кафедру про не допуск до виконання курсових робіт студентів, які не виконали навчальний план з дисциплін, що є базовими для виконання відповідних курсових робіт;
– разом з робочими планами розглядає, коригує і затверджує графік виконання курсових робіт, а у необхідних випадках розроблює і погоджує з керівником курсової роботи і індивідуальний план роботи студента;
– виносить на розгляд Вченої Ради факультету підсумки виконання курсових робіт та питання їх вдосконалення;
– у випадку необхідності інформує ректорат про хід виконання курсових робіт.

2.3. Обов’язки керівника курсової роботи

Організація курсової роботи з дисципліни «Безпека інформаційних систем та мереж» спеціальності 125 «Кібербезпека» спеціалізації «Безпека інформаційних і комунікаційних систем в економіці» покладається на кафедру інженерії програмного забезпечення та кібербезпеки.

Безпосереднє керівництво виконання курсової роботи здійснює керівник курсової роботи. Тема КР затверджується в перші два тижні курсової роботи. Керівник КР ознайомлює студентів з тематикою курсових робіт, проводить розподіл тем серед студентів, видає завдання на курсову роботу, та виконує такі роботи:

– готує індивідуальні завдання на курсові роботи, у яких визначає коло питань, які мають висвітлюватись у курсових роботах;
– заздалегідь розробляє графік виконання курсової роботи за формою, що наведена у таблиці 1 і контролює його виконання кожним студентом;
– у випадку необхідності контролює виконання студентом індивідуального графіка виконання курсової роботи;
– організовує і проводить консультації з питань виконання курсових робіт;
– перевіряє і візує до захисту (чи відхиляє) виконану, оформлену і підписану студентом курсову роботу;
– після завершення графіка виконання курсових робіт продовжує консультування, але переглядає і перевіряє вже повністю закінчену і оформлену курсову роботу.

Рекомендований графік роботи наведено в таблиці 2.1. Студент може корегувати графік в межах наведених дат, не змінюючи дати захисту.

Таблиця 1. – Рекомендований календарний план

№ з/п	Назва етапу роботи	Термін виконання (№ тижня)
1	Отримання завдання на курсову роботу, розробка і оформлення індивідуального завдання.	1-2 тижні
2	Аналіз предметної області, визначення мети роботи та загальної характеристики об’єкта дослідження. Визначення особливостей параметрів функціонування (метрик) об’єкта дослідження. Наведення порівняльної характеристики об’єкта дослідження, особливостей його функціонування у сукупності з іншими складовими обчислювальної системи. Подання електронного варіанта 1-го розділу.	3-4 тижні
3	Планування побудови програмно-технічного середовища та розробка основних вимог до розв’язання поставленої задачі. Визначення порядку проведення дослідження, можливого ступеня навантаження. Аналіз інструментів моніторингу об’єкта дослідження та середовища оточення, визначення порівняльної характеристики переваг та недоліків серед подібних програмних засобів. Визначення необхідності написання програмного коду та скриптів для досягнення поставленої мети. Подання електронного варіанта 2-го розділу	5-7 тижнів
4	Безпосереднє дослідження порушення доступності ресурсу: підготовка об’єкта дослідження та необхідних програмних засобів, встановлення операційної системи, віртуальних машин, інструментів навантаження та моніторингу. Отримання результатів виконання дослідження. Подання електронного варіанта 3-го розділу	7-9 тижнів
5	Аналіз та інтерпретація отриманих результатів дослідження. Проведення розрахунків описової статистики отриманих результатів дослідження, застосування методів статистичного аналізу та моделювання систем, отримання математичної моделі порушення доступності та визначення межі	10-13 тижнів

	доступності функціонування об’єкта дослідження. Подання електронного варіанта 4-го розділу	
6	Завершальне оформлення пояснювальної записки до курсової роботи. Захист курсової роботи	13-14 тижнів

Це не звільняє студента від повної відповідальності за обґрунтованість прийняти ним рішень, дотримання вимог нормативних документів і виконання календарного плану роботи.

Підпис керівника і членів комісії на титульному листі пояснювальної записки до курсової роботи свідчить не тільки про відповідність роботи всім нормативним вимогам, але й про підготовленість студента до вирішення конкретних інженерних задач.

2.4. Складові частини

Організаційно процес курсового проектування складається з наступних етапів:

- підготовчого, на якому студент отримує тему, узгоджує з керівником об’єкт проектування, особливості технічного завдання (ознайомлення зі станом проблеми, збирання фактичних матеріалів, проведення необхідних спостережень, досліджень тощо);
- основного, який починається одразу після узгодження технічного завдання й завершується тривалістю семестру. На цьому етапі робота повинна бути повністю виконана та перевірена керівником;
- заключного, який включає підготовку до захисту КР.

Основним документом, що представляють КР є пояснювальна записка. Текст пояснювальної записки до курсової роботи повинен бути викладений лаконічно, у обґрунтованому стилі. Не дозволяється переписування літературних джерел та використання не опрацьованих студентом Інтернет-оглядів.

Пояснювальна записка виконується на аркушах формату А4 згідно ДСТУ 3008-95. У випадку необхідності окремі ілюстрації можуть виконуватись на аркушах більших форматів.

2.5. Захист курсових робіт

В терміни, зазначені документом, курсова робота здається керівникові на перевірку. КР перевіряється по суті.

Для захисту КР кафедрою призначається комісія у складі не менше як двох викладачів. Захист КР проводиться у формі співбесіди зі з'ясуванням всіх питань, що виникли у керівника під час перевірки курсової роботи та членів комісії під час захисту.

На оцінку за КР впливають:

– якість виконання КР;
– компетентність та загальна ерудиція студента на запитання під час захисту.

Якщо студент подав на захист не самостійно виконану роботу, про що свідчить його некомпетентність у рішеннях та матеріалах проекти , ухвалою кафедри на подання керівника, КР до захисту перед комісією не допускається, що супроводжується записом "не допущений" у екзаменаційній відомості. Такий самий запис робиться у випадку, якщо КР не завершена на час захисту.

Захист курсових робіт відбувається на відкритому засіданні за затвердженим графіком у такому порядку:
– оголошується початок чергового відкритого захисту курсової роботи;
– зачитується прізвище студента, тема роботи;
– студент чітко, коротко, технічно правильно і лінгвістично грамотно доповідає про зміст виконаної роботи;
– учасники засідання та присутні задають запитання за змістом роботи, що стосуються теми роботи. Студент відповідає на кожне запитання чітко та за суттю;
– виступи інших учасників засідання, присутніх, керівника (за побажанням);
– оголошується закінчення захисту.

На доповідь дається 5 хвилин. За цей час необхідно продемонструвати результати виконаної роботи на комп’ютері, стисло викласти суть прийнятих рішень. Після закінчення доповіді викладач може задавати питання, призначення яких – уточнити рівень кваліфікації і ступень самостійності доповідача. На питання необхідно давати стислі прямі відповіді, при необхідності використовувати середовище моделювання КМ.

За результатами захисту комісія на закритому засіданні визначає оцінку, яка потім оголошується студенту. У результаті захисту курсової роботи виставляється оцінка в балах: 90-100, 82-89, 75-81, 69-74, 60-68, 35-59, 1-34.

3. СТРУКТУРА КУРСОВОЇ РОБОТИ

3.1. Обсяг курсової роботи

Курсова робота як оригінальне теоретично-прикладне дослідження мусить мати певну логіку побудови, послідовність і завершеність. Для успішного виконання КР необхідно чітко дотримуватись основних вимог до теоретичного рівня роботи, її змісту, структури, обсягу, форми викладання матеріалу, оформлення і захисту.

Виконання курсової роботи з дисципліни «Безпека інформаційних систем та мереж» розпочинається з титулки (Додаток А). Курсова робота виконується тільки за індивідуальними завданням.

Індивідуальне завдання на курсову роботу видається керівником. На бланку за формою, що наведена в Додатку Б обов'язково повинна бути вказана дата видачі завдання. Індивідуальне завдання засвідчується підписом керівника КР. Завдання не нумерується як розділ. Далі має бути правильно оформлена анотація (Додаток В), перелік умовних позначень, одиниць, символів, скорочень і термінів (Додаток Г), зміст роботи (Додаток Д), вступ (Додаток Ж).

Загальний обсяг пояснювальної записки – від 23 до 30 сторінок (не рекомендовано обсяг більший за 40 сторінок), причому технічна її частина, має містити не менш ніж 15 – 20 сторінок тексту з рисунками.

Бібліографічні описи в списку використаних джерел наводять відповідно до чинних стандартів з бібліотечної та видавничої справи відповідно ДСТУ ГОСТ 7.1:2006 "Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання". Приклад оформлення бібліографічного опису наведено у Додатку К.

Робота має бути виконана з урахуванням державних і галузевих стандартів (ДСТУ 3008−95. Документація. Звіти у сфері науки і техніки. Структура та правила оформлення).

Мова курсової роботи − державна, стиль − науковий, чіткий, без орфографічних і синтаксичних помилок.

Пояснювальна записка має відповідати індивідуальному завданню, а її оформлення – чинним (на момент виконання розробки, з урахуванням всіх офіційних змін, введених в дію) державним стандартам.

Пояснювальна записка має таку структуру.

1. Вступна частину, яка містить:
 - титульний аркуш;
- індивідуальне завдання;
- анотацію;
- зміст.
2. Основна частина, яка складається зі:
- вступу;
- викладу суті курсової роботи;
- висновків та пропозицій;
- списку використаних джерел.
3. Додатки, які розміщують після основної частини пояснювальної записки КР.

<u>Рекомендується така структура курсової роботи:</u>

1. Титульний лист (Додаток А)
2. Індивідуальне завдання на курсовий проект за формою (Додаток Б)
3. Анотація (Додаток В)

4. Перелік умовних позначень, одиниць, символів, скорочень і термінів (Додаток Г)
4. Зміст роботи (Додаток Д)
5. ВСТУП (Додаток Ж)
6. РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ…
7. РОЗДІЛ 2. ЗАГОЛОВОК ДРУГОГО РОЗДІЛУ
    2.1. Заголовки підрозділів
8. РОЗДІЛ 3. ЗАГОЛОВОК ТРЕТЬОГО РОЗДІЛУ …
    3.1. Заголовки підрозділів
9. Висновки та пропозиції;
10. Список використаних джерел (приклад у Додатку К);
11. Додатки.

Змістовне наповнення пояснювальної записки та графічної частини – це результат самостійної – творчої роботи студента з питань, сформульованих у завданні на курсову роботу.

3.2. Вимоги до змісту розділів, оформлення та обсягу

До *пояснювальної записки (ПЗ*) необхідно включати матеріал, який безпосередньо відноситься до конкретної комп'ютерної мережі, яка підлягає моделюванню, у відповідності до завдання, згідно варіанту. Не рекомендується робити великі реферативні огляди. При необхідності можна робити посилання на відповідну літературу. Основний зміст записки – це обґрунтування прийнятих рішень, згідно затвердженої назви. При цьому треба мати на увазі, що записку складають тоді, коли розробку комп'ютерної мережі завершено, всі рішення прийнято, всі деталі є відомими, є кінцевий результат, і саме його необхідно привести у записці разом з аргументацією вибору рішень, необхідними розрахунками, таблицями, рисунками, діаграмами, графіками та іншими матеріалами, які обґрунтовують прийняті рішення.

Пояснювальна записка не повинна бути перевантаженою за рахунок малоінформативного оглядового матеріалу, для скорочення обсягу якого рекомендується робити посилання на використані джерела інформації та менше їх цитувати. Доцільно вживати однакову термінологію. При перекладі з іноземної на українську мову невідомих термінів доцільно використовувати відповідні словники.

Не допускається дослівне переписування матеріалів з будь-яких джерел.

При необхідності дозволяється коротке цитування використаного матеріалу та посилання на джерела інформації.

Приблизний рекомендований обсяг кожного розділу наведено нижче. Назви розділів у конкретній роботі можуть відрізнятись від наведених далі, послідовність розташування розділів може бути іншою, але в цілому у

пояснювальній записці рекомендовано висвітлити всі питання.

В анотації у реферативному стилі наводиться інформація про зміст та результати, що отримані в курсової роботі. Як розділ анотація не нумерується.

Зміст курсової роботи може займати 1–1,5 сторінки. В ньому записуються назви всіх розділів і підрозділів (параграфів) із зазначенням початкових сторінок. Назви розділів і підрозділів мають бути стислими і зрозумілими, літературно грамотними, тісно пов'язаними з назвою роботи, але не повторювати її. Усі назви повинні бути записані так само як вони сформульовані в КР. Визначення сторінок обов'язкове. Зміст характеризує структуру КР. Як розділ зміст не нумерується.

У вступі студент повинен висвітлити стан питання, яке розглядається, обґрунтовувати необхідність і можливість його вирішення, описати зв'язок з виробничими задачами, а також обґрунтувати актуальність теми роботи та сформулювати основну мету, визначити об'єкт дослідження, предмет дослідження, огляд програмних продуктів, існуючих алгоритмів, огляд і посилання на закони щодо захисту інформації, результат аналізу джерел по темі курсової роботи, тощо Вступ має бути коротким (1-2 сторінки) і чітким. Його не слід перевантажувати загальними фразами. Головне, щоб було зрозуміло, чому присвячена робота, які завдання автор поставив сам для себе. Вступ як розділ не нумерується.

У першому розділі (3-4 сторінки) ПЗ необхідно провести огляд та аналіз предметної області. Студент повинен визначити коло задач, які необхідно вирішити в курсовій роботі, а також сформулювати технічне завдання згідно діючих стандартів та оформити його окремим підрозділом.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ … НА ОБ’ЄКТІ…

Метою розділу 1 є здійснення детального аналізу сфери діяльності об'єкта захисту (підприємства/організації/закладу) та виникнення можливих проблем із захисту інформації у процесі використання сучасних технологій під час ведення бізнесу.

Необхідно коротко описати напрями діяльності об'єкта захисту (підприємства, організації, закладу); визначити проблеми із захистом інформації, що мають/можуть мати місце у процесі використання сучасних технологій обробки даних; які заходи із захисту інформації може бути застосовано та підрозділ, якому делеговано ці функції; розробити схему інформаційних вразливостей організаційної структури управління підприємством.

Приклади предметної області:

Захист банківських ресурсів в автоматизованій банківській системі.

Захист інформації в корпоративних мережах.

Захист інформації у віртуальних приватних мережах.

Захист фінансової інформації в інформаційно-телекомунікаційних системах.
Захист інформації від несанкціонованого доступу.
Захист інформації в автоматизованих системах.
Захист інформації в аналітичних системах.
Захист інформації в системах електронного документообігу.
Захист інформації в системах мобільного зв'язку.
Захист інформації в системах електронної пошти.
Захист інформації в локальних мережах …

1.1. Коротка характеристика сфери діяльності об'єкта захисту (назва об'єкта захисту).

Необхідно коротко описати вибрані для дослідження напрями діяльності об'єкта захисту (підприємства, організації, закладу);

1.2.Характеристика інформації, що підлягає захисту.

Необхідно перелічити за підрозділами об'єкта назви документів на паперових та електронних носіях, що підлягають захисту, розробити схему інформаційних вразливостей організаційної структури управління підприємством, визначити проблеми із захистом інформації, що мають/можуть мати місце у процесі використання сучасних технологій обробки даних.

1.3 Характеристика можливих заходів із захисту інформації, які може бути застосовано

У другому розділі (4-5 сторінок) виконується планування встановлення програмно-технічного середовища та дотримання основних вимог для розв'язання поставленої задачі, визначення порядку проведення досліджень,

РОЗДІЛ 2. АНАЛІЗ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В <НАЗВА ОБ'ЄКТА ЗАХИСТУ> (АНАЛІЗ УМОВ ФУНКЦІОНУВАННЯ ТА СУЧАСНИХ ЗАГРОЗ ІНФОРМАЦІЇ)

Метою розділу 2 є здійснення детального аналізу загроз інформаційній безпеці об'єкта захисту та розроблення моделей загроз і порушника з описом системи захисту інформації, інженерно-технічних, апаратних та програмних засобів.

2.1. Побудова моделі загроз.

Перелік загроз інформаційній безпеці необхідно розглянути за цільовою ознакою класифікації та описом складових інформаційних потоків, критичних до модифікування. Для системи визначити перелік класів загроз за:
1) природою виникнення;
2) ступенем навмисності;
3) безпосереднім джерелом загроз;
4) станом джерела загроз;
5) мірою залежності від активності інформаційної системи (ІС);

6) мірою впливу на ІС;
7) етапами доступу користувачів або програм до ресурсів ІС;
8) способом доступу до ресурсів ІС;
9) поточним місцем розміщення інформації, що зберігають і обробляють в ІС.

2.2. Побудова моделі порушника.

З урахуванням технології обробки інформації та побудови моделі загроз інформації необхідно розробляти модель порушника, яка має бути адекватною реальному порушнику для певної ІС.

Модель порушника має визначати:
1) можливу мету порушника та її градацію за ступенем небезпеки для ІС;
2) категорії осіб, із яких може бути порушник;
3) можлива кваліфікація порушника;
4) можливий характер його дій.

2.3. Оцінювання ризику реалізації загроз у комунікаційних системах.

2.4. Інженерно-технічні, апаратні та програмні засоби захисту інформації в…(назва об'єкта захисту).

2.4.1. Опис складу фізичних об'єктів, механічних, електричних та електронних пристроїв, елементів конструкцій будівель, засобів пожежогасіння та інших засобів, що забезпечують на об'єкті захисту:

- захист території та приміщень від проникнення порушників;
- захист апаратних засобів і носіїв інформації від розкрадання;
- запобігання можливості віддаленого (із-за меж території, що охороняють) відеоспостереження (підслуховування) за роботою персоналу і функціонуванням технічних засобів;
- запобігання можливості перехоплення побічних електромагнітних випромінювань і наведень (ПЕМВН), викликаних працюючими технічними засобами і лініями передавання даних;
- організацію доступу у приміщення співробітників;
- контроль над режимом роботи персоналу;
- контроль над переміщенням співробітників у різних виробничих зонах;
- протипожежний захист приміщень; …

2.4.2. Опис апаратних пристроїв, а саме:

- пристроїв для введення інформації, що ідентифікує користувача (магнітних і пластикових карт, відбитків пальців і т. ін.);
- пристроїв для шифрування інформації;
- пристроїв для перешкоджання несанкціонованому вмиканню робочих станцій і серверів (електронні замки та блокатори).

2.4.3. Опис програмних засобів захисту інформації:

- програми ідентифікації й автентифікації користувачів корпоративної мережі;
- програми розмежування доступу користувачів до ресурсів корпоративної мережі;
- програми шифрування інформації;
- програми захисту інформаційних ресурсів (системного і прикладного програмного забезпечення, баз даних, комп'ютерних засобів навчання і т. ін.) від несанкціонованої зміни, використання та копіювання.
- програми знищення залишкової інформації (у блоках оперативної пам'яті, тимчасових файлах і т. ін.);
- програми аудиту (ведення реєстраційних журналів) подій, пов'язаних із безпекою корпоративної мережі, для забезпечення можливості відновлення і доведення факту існування цих подій;
- програми імітації роботи з порушником (відволікання його на отримання нібито конфіденційної інформації);
- програми тестового контролю за захищеністю корпоративної мережі та ін.

Третій розділ (5-15 сторінки) передбачає безпосереднє виконання дій (операцій), що були передбачені у попередньому розділі що призводять до порушення доступності ресурсу. До таких дій належать підготовка об’єкта дослідження та необхідних програмних засобів, встановлення операційної системи, віртуальних машин, інструментів навантаження та моніторинг. Виконується аналіз та інтерпретація отриманих результатів дослідження, де проводяться розрахунки описової статистики отриманих результатів дослідження, застосування методів статистичного аналізу та моделювання систем, отримання математичної моделі порушення доступності та визначення межі доступності функціонування об’єкта дослідження. В цьому випадку можуть бути використані методи параметричної та непараметричної статистики, багатовимірного аналізу, кореляційного та регресійного аналізів, компонентного аналізу (аналізу головних компонент) тощо.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ДОДАТКОВИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ІТС… (НАЗВА ОБ'ЄКТА ЗАХИСТУ)

У практичній частині необхідно провести дослідження по наступних пунктах:

3.1. Методи і засоби захисту інформації, що впроваджені в інформаційну систему підприємства. Наявність (відсутність) служби з питань захисту інформації.

3.2 Вибір, обґрунтування та опис функціонування додаткових програмно-апаратних засобів захисту інформації

3.3 Розробка програмних модулів захисту інформації (CMD, PowerShell).

У висновках та пропозиціях (1-2 сторінки) формулюються основні результати, які отримані під час виконання курсової роботи. В реферативній формі повинні бути описані результати, отримані студентом на кожному з етапів виконання роботи, а також висновків щодо досягнення мети курсової роботи, перспективи розвитку даної галузі тощо. Як розділ не нумерується.

У Списку використаних джерел наводиться перелік використаних джерел, на які були посилання в тексті. Список повинен формуватися в порядку посилань за текстом і вміщувати бібліографічні відомості офіційно виданих книжок, статей, патентів, депонованих рукописів тощо. Як розділ перелік літератури не нумерується.

У додатки включають логічні схеми, а також інші документи. Крім цього, в додатки помішуються таблиці, графіки та методики, які з якихось причин не увійшли до пояснювальної записки, але потрібні для пояснень. Як розділ додатки не нумеруються, але кожен з додатків нумерується великими літерами алфавіту згідно ДСТУ 3008-95, оскільки до додатків помішуються документи, що мають самостійну нумерацію сторінок, то різна нумерація (спільна для всієї пояснювальної записки) зберігається.

4. ВИМОГИ ДО ОФОРМЛЕННЯ ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

4.1. Загальні вимоги

Курсова робота має бути виконана й оформлена з додержанням усіх технічних вимог до наукових робіт. Текст роботи має бути набраний на комп'ютері в текстовому редакторі *MS Word* на одному боці аркуша білого паперу формату А4. Шрифт Times New Roman, 14 пт, через 1,5 інтервалу, текст вирівнюється по ширині аркуша. Можна також подати таблиці та ілюстрації на аркушах формату А3.

Текст розміщується на сторінці, яка обмежується полями: лівим − не менш як 30 мм, правим − не менш як 10 мм, верхнім − не менш як 20 мм, нижнім — не менш як 20 мм. Відстань між заголовком і текстом має бути в межах 15-20 мм.

Текст ПЗ пишеться літературною державною мовою. У тексті ПЗ не дозволяється: вживати звороти розмовної мови; вживати застарілі та жаргонні терміни і вислови; вживати скорочені слова, крім встановлених стандартами скорочень. У тексті ПЗ, за винятком формул, таблиць і

рисунків, не допускається: вживати математичний знак мінус (-) перед від'ємними величинами (треба писати слово "мінус"); вживати без числових значень знаки >, <, =, :, %, №.

У ПЗ треба використовувати одиниці СІ. Якщо значення приведено в інших одиницях, переведення їх в одиниці СІ обов'язкове лише за умови викладення найважливіших положень ПЗ. Якщо в тексті ПЗ наводиться ряд числових значень в однакових одиницях, то позначення одиниці виміру зазначають тільки після останнього числового значення, наприклад: 1, 2, 3 м; або від 5 до 10 мм. Одиниці вимірювання від числових величин відокремлюють нерозривним пробілом (Ctrl+Shift+Space).

Числові значення величин треба відокремлювати від десяткової частини комою, наприклад: 7,5; 8,75; 10,00. Помилки та графічні неточності допускається виправляти підчищенням або зафарбовуванням білою фарбою і нанесенням на тому ж місці або між рядками виправленого зображення машинним способом або від руки. Виправлене повинно бути чорного кольору. Прізвища, назви установ, організацій, фірм та інші власні назви у ПЗ наводять мовою оригіналу. Допускається транслітерувати власні назви і наводити назви організацій у перекладі на мову звіту, додаючи (при першій згадці) оригінальну назву. Структурні елементи «РЕФЕРАТ», «ЗМІСТ», «ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ», «ВСТУП», «ВИСНОВКИ ТА ПРОПОЗИЦІЇ», «СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ» не нумерують, а їх назви використовують за заголовки структурних елементів. Заголовки структурних елементів ПЗ слід розташовувати посередині рядка і друкувати великими літерами без крапки в кінці, не підкреслюючи

Список позначень і прийнятих скорочень обов'язково має бути окремим підрозділом роботи, якщо при її написанні застосовується спеціальні скорочення, символи та терміни. Цей розділ має передувати викладенню основної частини курсової роботи.

Скорочення, символи та терміни розміщуються стовпчиком, у якому зліва розташовані символи та спеціалізовані терміни, а праворуч – їх розшифрування.

Текст основної частини ПЗ поділяють на розділи відповідно до завдання і структури КР. Розділи і підрозділи повинні мати заголовки. Пункти і підпункти можуть мати заголовки.

Якщо заголовок складається з двох і більше речень, їх розділяють крапкою. Перенесення слів у заголовку розділу не допускається. Відстань між заголовком і подальшим чи попереднім текстом має бути не менше, ніж один порожній рядок. Не допускається розміщувати назву підрозділу, а також пункту й підпункту в нижній частині аркуша, якщо після неї розміщено тільки один рядок тексту.

Аркуші ПЗ слід нумерувати арабськими цифрами, додержуючись наскрізної нумерації впродовж усього тексту. Номер аркушу проставляють у відповідному полі основного напису.

Титульний аркуш та завдання на курсову роботу включають до загальної нумерації аркушів ПЗ. Номер на титульному аркуші та завданні не проставляють. Аркуш, розміщений після завдання на курсову роботу, нумерується цифрою 4.

Ілюстрації й таблиці, розміщені на окремих аркушах, включають до загальної нумерації аркушів ПЗ.

Кожен структурний елемент ПЗ починають з нового аркушу. Оформлення аркушу структурного елементу ПЗ проводиться відповідно до таких вимог.

4.2. Заголовки

Розділи, підрозділи мусять мати заголовки, що чітко й коротко відображають їхній зміст.

Заголовки розділів, підрозділів і пунктів слід друкувати з абзацним відступом з великої літери без крапки в кінці та без підкреслень.

Якщо заголовок складається з двох речень, їх відокремлюють крапкою. Перенесення слів у заголовку розділу не допускається. У разі використання набірних друкарських форм заголовки розділів і підрозділів слід виділяти шрифтом.

4.3. Переліки

У тексті пунктів або підпунктів можуть бути переліки. Перед кожною позицією переліку слід ставити дефіс або (за необхідності послатися в тексті на один із переліків) малу літеру, після якої ставлять дужку. Для подальшої деталізації переліку необхідно використовувати арабські цифри, після яких ставлять дужку.

Перелік першого рівня деталізації друкують малими літерами з абзацного відступу, другого рівня − з відступом відносно місця розташування переліків першого рівня.

Приклад:

а)_____

б)_____

1)_____

2)_____

в)_____

4.4. Графічний матеріал

Графічний матеріал – рисунки (схеми, діаграми тощо) розміщують у КР для встановлення властивостей або характеристик об'єкта, а також для

ліпшого розуміння тексту роботи. На графічний матеріал мають бути посилання в тексті курсової роботи.

Графічний матеріал розміщують безпосередньо після тексту, в якому про нього згадується вперше, або на наступній сторінці, а за необхідності – у додатку.

Таблиці, що доповнюють графічний матеріал, подають після графічного матеріалу.

Графічний матеріал може мати тематичну назву, яку розміщують під ним. За необхідності під графічним матеріалом наводять пояснювальні дані. Слово «рисунок» і назву подають після пояснювальних даних. Графічний матеріал (за винятком графічного матеріалу додатків) слід нумерувати арабськими цифрами порядковою нумерацією в межах розділу. Якщо рисунок один, його позначають “Рис. 1”. Номер рисунка складається з номерів розділу та порядкового номера рисунка, відокремлених крапкою (Рис. 1.1).

Графічний матеріал кожного додатка позначають окремою нумерацією арабськими цифрами з додаванням перед цифрою позначення додатка (Рис. В.3).

4.5. ФОРМУЛИ

Формули мають нумеруватися арабськими цифрами порядковою нумерацією в межах розділу, які друкують на рівні формули праворуч у круглих дужках.

Номер формули складається з номера розділу і порядкового номера формули, відокремлених крапкою.

Приклад:

(3.1), (3.3).

Посилання в тексті на порядкові номери формули дають у дужках.

Приклад:

... у формулі (1.1).

Формули в додатках нумерують окремо арабськими цифрами в межах кожного додатка з додаванням перед цифрою позначення додатка.

Приклад:

... у формулі (В. 1).

У формулі як символи фізичних величин слід застосовувати позначення, встановлені відповідними стандартами або іншими документами.

Пояснення символів і числових коефіцієнтів, що входять до формули, якщо вони не пояснювалися в тексті, мають бути наведені безпосередньо під формулою. Пояснення кожного символу слід давати з нового рядка в тій послідовності, в якій символи наведено у формулі. Перший рядок пояснення має починатися словом “де” без двокрапки.

Формули, що подаються одна за одною і не розділені текстом, відокремлюють комою.

4.6. Додатки

Матеріал, що доповнює положення курсової роботи, допускається розміщувати в додатках. Додатками можуть бути: графічний матеріал, таблиці великого формату, розрахунки, опис алгоритмів і програм задач, що розв'язуються на ПК тощо.

Додатки можуть бути обов'язковими та інформаційними. Інформаційні додатки можуть мати рекомендований або довідковий характер.

Додатки позначають великими літерами української абетки, починаючи з А, за винятком літер Ґ, Є, З, І, Ї, Й, О, Ч, Ь. Після слова "Додаток" друкують літеру, що позначає його послідовність.

Допускається позначення додатків літерами латинської абетки за винятком літер I та O.

У разі повного використання літер української та латинської абеток допускається позначення додатків арабськими цифрами.

Якщо у КР один додаток, то він позначається "Додаток А".

Кожний додаток слід починати з нової сторінки із зазначенням угорі в середині сторінки слова "Додаток" і його позначенням, а під ним у дужках для обов'язкового додатка друкують слово "обов'язковий", а для інформаційного – "рекомендований" чи "довідковий". Додаток мусить мати заголовок, який друкують симетрично відносно тексту з великої літери окремим рядком.

Текст кожного додатка за необхідності може бути поділений на розділи, підрозділи, пункти, підпункти.

Запозичена з літературних чи статистичних джерел інформація (формули, таблиці, схеми, графіки, висновки тощо) потребує обов'язкових посилань (у квадратних дужках) на порядковий номер джерела у списку використаних джерел та номери сторінок, з яких узято інформацію.

4.7. Ілюстрації

Усі ілюстрації у записці у вигляді креслень, ескізів, схем, графіків, діаграм, фотографій та ін. називаються рисунками. Ілюстрації можуть бути розташовані на окремих аркушах або безпосередньо в тексті записки.

Ілюстрації слід розміщувати у ПЗ безпосередньо після тексту, де вони згадуються вперше, або на наступній сторінці. На усі ілюстрації повинні бути посилання в тексті ПЗ, наприклад: «наведено на рисунку 6.1».

Ілюстрації повинні мати назву, яку розміщують під ілюстрацією

(див. рисунок 1). За необхідності під ілюстрацією розміщують пояснювальні дані. Ілюстрація позначається словом «Рисунок», яке разом з назвою ілюстрації розміщують після пояснювальних даних. Ілюстрації слід нумерувати арабськими цифрами порядковою нумерацією в межах розділу, за винятком ілюстрацій, наведених у додатках. Номер ілюстрації складається з номера розділу і порядкового номера ілюстрації, відокремлених крапкою, наприклад, рисунок 2.16 − шістнадцятий рисунок другого розділу.

Рисунок 4.1 – Приклад оформлення ілюстрацій

Після номеру ставиться тире (−), а після назви крапка не ставиться.

Ілюстрації і назва ілюстрації розміщуються по центру сторінки. Від основного тексту зверху і знизу відділяються пустим рядком.

Якщо ілюстрація не вміщується на одній сторінці, можна переносити її на інші сторінки, вміщуючи назву ілюстрації на першій сторінці, пояснювальні дані − на кожній сторінці, і під ними позначають: «Рисунок __, аркуш __».

Якщо ілюстрація велика, то її дозволяється розміщувати на аркуші А4 в альбомній орієнтації, при цьому найменування розміщують під рисунком, а рамка основного напису залишається в стандартному положенні (вздовж короткої сторони аркуша А4). Не прийнято завершувати розділ рисунком.

4.8. Таблиці

Таблицю слід розташовувати безпосередньо після тексту, у якому вона згадується вперше, або на наступній сторінці.

Таблиці слід нумерувати арабськими цифрами порядковою

нумерацією в межах розділу, за винятком таблиць, що наводяться у додатках.

Номер таблиці складається з номера розділу і порядкового номера таблиці відокремлених крапкою. Номер таблиці від назви виділяють тире. Приклад оформлення таблиці приведено на рисунку 4.2.

Таблиця 3.1 - Основні етапи виконання курсової роботи

№ та назва етапу	Середній час виконання стадії (етапу), год.	
	Інженер	Керівник
1. Розробка та затвердження технічного завдання.	6	2
2. Аналіз технічного завдання, збір необхідної інформації по розробці, техніко-економічний аналіз.	7	1
3. Проектування локальної мережі	15	4
4. Організація кабельної структури мережі	48	4
5. Налаштування апаратного забезпечення мережі	62	11
6. Організаційно-економічна частина	4	1
7. Охорона праці та безпека в надзвичайних ситуаціях	4	1
8. Екологія	4	1
Разом	150	25

Рисунок 4.2 – Приклад оформлення таблиць.

Таблиці (за винятком таблиць у додатках) слід нумерувати арабськими цифрами порядковою нумерацією в межах розділу. Номер таблиці складається з номеру розділу і порядкового номера таблиці, відокремлених крапкою, наприклад, “Таблиця 3.1” − перша таблиця третього розділу.

Таблиці кожного додатка позначають окремою нумерацією арабськими цифрами з додаванням перед цифрою позначення додатка.

На всі таблиці мають бути посилання в тексті, які складаються зі

слова “таблиця” із зазначенням її номера.

Заголовки стовпців і рядків таблиці слід друкувати з великої літери, підзаголовки стовпців з малої, якщо вони е продовженням заголовка, або з великої, якщо вони мають самостійне значення. У кінці заголовків і підзаголовків таблиць крапки не ставлять, заголовки і підзаголовки стовпців друкують в однині.

Таблиці ліворуч, праворуч і знизу, як правило, обмежують лініями.

Розділення заголовків і підзаголовків боковика і стовпців діагональними лініями не допускається.

Горизонтальні та вертикальні лінії, що розмежовують рядки таблиці, можна не креслити, якщо відсутність таких не ускладнює користування таблицею.

Заголовки стовпців, як правило, друкують паралельно рядкам таблиці. За необхідності допускається перпендикулярне розміщення заголовків стовпців.

Головку таблиці треба відокремлювати лінією від тексту таблиці.

Допускається розміщення таблиці вздовж довгого боку аркуша.

Якщо рядки або стовпці таблиці виходять за формат сторінки, то таблицю ділять на частини, які розміщують одна під одною або поряд, при цьому в кожній частині таблиці повторюють її головку й боковик.

У разі поділу таблиці на частини допускається її головку або боковик заміняти відповідно номерами стовпців і рядків. При цьому нумерують арабськими цифрами стовпці і (або) рядки першої частини таблиці.

Якщо в кінці сторінки таблиця переривається і її продовження буде на наступній сторінці, то в першій частині таблиці нижню горизонтальну лінію, що обмежує таблицю, не креслять.

5. КРИТЕРІЇ ОЦІНЮВАННЯ КУРСОВОЇ РОБОТИ

Оцінка за курсову роботу складається із суми балів, які виставляються комісією на основі розгляду змісту ПЗ і графічного матеріалу та за підсумком усного захисту перед комісією основних положень, які розглянуті в курсовій роботі. Підсумкова оцінка знань, умінь та навичок студента, набутих при проектуванні КР, встановлюється за 100-бальною шкалою:

- 90-100;
- 82-89;
- 75-81;
- 69-74 ;
- 60-68;
- 35-59;

- 1-34.

6. ПІДГОТОВКА ДО ЗАХИСТУ КУРСОВОЇ РОБОТИ

Після завершення написання курсової роботи студент подає та реєструє роботу на кафедрі із зазначенням строку здачі у спеціальному журналі (під розпис студента).

На курсову роботу має бути надано відгук наукового керівника. Керівник вирішує питання про допуск студента до захисту, роблячи відповідний запис на титульному аркуші курсової роботи.

У разі невідповідності курсової роботи вимогам даних рекомендацій керівник курсової роботи може не допустити студента до захисту роботи.

Рішення керівника щодо недопущення студента до захисту має бути затверджене на засіданні кафедри.

Якщо робота допущена до захисту студент повинен ознайомитись із відзивом і підготуватись до захисту. При цьому він повинен підготувати відповіді на питання згадані у відгуку й показати усунені недоліки.

Захист курсової роботи проводиться перед початком екзаменаційної сесії. Процедуру з захисту курсової роботи організовує комісія у складі принаймні трьох викладачів у присутності всіх студентів групи. Процедура захисту передбачає стислий виклад студентом головних проблем дослідження роботи та їх рішення упродовж 10-15 хвилин, відповіді на запитання членів комісії.

При оцінці курсової роботи береться до уваги:

- ✓ зміст і складність роботи;
- ✓ якість виконання;
- ✓ відповідність роботи щодо її оформлення;
- ✓ набуті студентом навички пов’язувати теоретичні знання з питаннями їх практичного застосування;
- ✓ повнота та точність відповідей на поставлені запитання.

Оцінка виконання КР виставляється у заліковій книжці студента, реєструється на спеціальному бланку та на титульному листі.

Студент, який отримав на захисті незадовільну оцінку - до екзамену з дисципліни «Безпека інформаційних систем та мереж» не допускається.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99.
2. Остапов С.Е., Євсеєв С.П., Король О.Г., Технології захисту інформації. Навчальний посібник. Чернівці.- Видавничий дім «Родовід», 2014. – 471с.
3. Кавун С.В. Інформаційна безпека: підручник. Харків : ХНЕУ, 2013. - 213с.
4. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах: навч. посібник. – К., 2013. – 435с., іл.160.
5. Єсін В. І. Безпека інформаційних систем і технологій: навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632с.

Додатковий

6. Концепція (основи державної політики) національної безпеки України від 21 грудня 2000 року №2171-111.
7. Інструкція про порядок обліку і зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави від 27 листопада 1998 року № 1893.
8. Положення про порядок здійснення криптографічного захисту інформації в Україні від 22 травня 1998 року № 505/98.
9. Антонюк А., Жора В. Моделювання доступу та каналів витоку в інформаційних системах/Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. - №3.160 С.
10. *Пашкова А. Т. Інформаційна безпека як складова національної безпеки А. Т. Пашкова // Безпека життєдіяльності. – Київ, 2014. – № 11. – С. 34-36.*
11. *Полянська В. Кібернетична безпека України в умовах розвитку глобальної інформаційної системи / В. Полянська // Підприємництво, господарство і право. – Київ, 2013. – № 7 (211). – С. 48-50.*
12. A.Menezes,
P. van Oorshot, S.Vanstone. Handbook of Applied Cryptography.
CRC Press Inc, 2015, 780 p.
13. Г.В.Кузнецов, В.В.Фомичов, С.О.Сушко. Математичні основи криптографії: Ч.1. Дніпропетровськ: Національний гірничий університет, 2014,391с.
14. В.С. Сідак, В.Ю. Артемов. Забезпечення інформаційної безпеки в країнах НАТО та ЄС. К. КНТ. 2012, 160с.

Internet-ресурси

15. Защита информации – режим доступу: *http://www.bseu.by/it/tohod/lekcii9_2.htm*
16. Захист інформації – режим доступу: *http://www.warning.dp.ua/tel28.htm*
17. Безпека на прикладному рівні – режим доступу: *http://www.dut.edu.ua*
18. IEEE computer society. SWEBOK – режим доступу: *http://www.computer.org/portal/web/swebok/htmlformat*
19. Process Models in Software Engineering – режим доступу: *http://www.ics.uci.edu/~wscacchi/Papers/SE-Encyc/Process-Models-SE-Encyc.pdf*
20. Technical writing for software engineers – режим доступу: *http://www.dtic.mil/dtic/tr/fulltext/u2/a223872.pdf*

**Курсивом зазначені джерела, що є в наявності в бібліотеці КНТЕУ*

ДОДАТКИ

ДОДАТОК А

Міністерство освіти та науки України
Київський національний торговельно-економічний університет
Факультет інформаційних технологій
Кафедра інженерії програмного забезпечення та кібербезпеки

КУРСОВА РОБОТА
З ДИСЦИПЛІНИ
«БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ»
НА ТЕМУ:

_____

(назва теми)

Студента факультету _____
групи_курсу_____
_____
Прізвище, ім'я, по-батькові (підпис)

Науковий керівник_____
_____
(підпис)

Кількість балів: _____

Члени комісії:

_____

_____

_____

Київ 20__

ДОДАТОК Б

Київський національний торговельно-економічний університет

Кафедра _____

Дисципліна _____

Курс _____ Група _____Семестр_____

ЗАВДАННЯ
на курсову роботу студента

_____

(прізвище, ім'я, по батькові)

1. Тема курсової роботи_____

_____

_____

_____

_____

2. План курсової роботи_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

3. Перелік графічного матеріалу _____

_____

_____

_____

4. Термін подання студентом завершеної курсової роботи (проекту) на кафедру _____

5. Термін захисту курсової роботи (проекту)_____

6. Дата видачі завдання _____

Студент_____

(підпис)

Науковий керівник _____ _____

(підпис) (прізвище, ім'я, по батькові)

Завідувач кафедри _____ _____

(підпис) (прізвище, ім'я, по батькові)

ДОДАТОК В

Приклад анотації

АНОТАЦІЯ

Курсова робота виконана студентом групи ФІТ-3-12 Івановим Іваном Івановичем на тему «Захист комерційної таємниці на підприємстві». Робота складається зі вступу, трьох розділів, висновків та пропозицій, списку використаних джерел, який складається з 57 найменувань, 2 додатків. Робота містить 5 рисунків і 8 таблиць. Загальний обсяг роботи становить 35 сторінок

У курсовій роботі був проведений детальний аналіз термінологічної проблеми у сфері інформаційної безпеки та на його основі запропоновані власні визначення ключових елементів термінології. Проаналізовано динаміку використання визначених термінів у публікаціях різних напрямів та проведено детальний аналіз різними методами отриманих результатів. Проведено порівняльний аналіз відповідних термінів у сфері кібербезпеки.

Темою роботи є системний аналіз категорії «загроза» в інформаційній безпеці.

Метою даної роботи є дослідження категорії «загроза», вирішення термінологічної проблеми у сфері інформаційної безпеки та встановлення чіткого розділення між кібернетичною сферою.

Об’єкт дослідження – використання визначеної термінології у публікаціях різних напрямів та нормативно-правових документах. Предметом дослідження є контекст, в якому використовуються визначені терміни та динаміка популярності їх вживання.

Методами дослідження є: інтелектуальний аналіз тексту (Text Mining), розвідковий аналіз, порівняльний аналіз, RS-аналіз.

Ключові слова: інформаційний простір, інформаційна безпека, інформаційна загроза, інформаційний ризик, термінологія, аналіз, результати.

ДОДАТОК Г

Приклад оформлення

Перелік умовних позначень, символів, одиниць, скорочень і термінів

ІС	–	інформаційна система
ІТ	–	інформаційні технології
ІТС	–	інформаційно-телекомунікаційна система
ЦОД	–	центр обробки даних
ПЗ	–	програмне забезпечення
IoT	–	інтернет речей
IoE	–	інтернет всього
НСД	–	несанкціонований доступ
КЦД	–	конфіденційність, цілісність, доступність
КСЗІ	–	комплексна система захисту інформації
ПБ	–	політика безпеки
ІБ	–	інформаційна безпека
ЕМВ	–	електромагнітне випромінювання
ПЕМВ	–	побічне електромагнітне випромінювання
ТЗР ПЕМВН	–	технічні засоби розвідки побічних електромагнітних випромінювань і наведень
ОС	–	операційна система
ЕОМ	–	електронна обчислювальна машина
ПК	–	персональний комп’ютер
LAN	–	локальна комп'ютерна мережа
WAN	–	глобальна мережа
UNIX	–	сімейство операційних систем
HTTP	–	протокол передачі гіпертексту та інших типів даних
MAC	–	унікальний ідентифікатор обладнання для комп'ютерних мереж

ДОДАТОК Д

ЗМІСТ

ДОДАТОК Ж

Структура вступу до курсової роботи:

1. **Вступна частина** (не більше 1-го абзацу або 2-3 пропозиції) – описується загальний стан розглянутої теми.

2. **Актуальність дослідження** – тут слід написати про важливість вивчення даної теми в даний час. Тобто пояснити, чому ви вибрали саме це тему і що дозволить зробити її вивчення.

3. **Актуальність та новизна**: – пишуть для того, щоб розуміти, що для досягнення мети роботи слід вивчити, описати, показати, визначити, встановити, досліджувати, розглянути, розробити, розкрити, висвітлити, виявити, проаналізувати, довести, узагальнити що-небудь.

4. **Мета курсової роботи**. Це може бути: вивчення, опис, визначення, встановлення, дослідження, розгляд, розробка, розкриття, освітлення, виявлення, аналіз, узагальнення чого-небудь.

5. **Об'єкт і предмет дослідження**. Об'єкт включає в себе предмет, а не навпаки. Адже предмет говорить про більш вузький сектор дослідження і змушує нас конкретизувати область дослідження.

6. **Предметом дослідження** є контекст, в якому використовуються визначені терміни та динаміка популярності їх вживання.

7. **Методами дослідження** є: інтелектуальний аналіз

8. **Огляд літератури.** У цій частині введення слід вписати тих авторів, праці яких використовувалися при написанні курсової, і коротко описати, що вони вивчали. При цьому важливо вказати також і тих авторів, які були рекомендовані науковим керівником.

9. **Опис структури курсової роботи.** Тут варто вказати всі розділи, які містить курсова робота і що в них розглянуто.

Приклад вступу до курсової роботи подано нижче.

ВСТУП

У сучасному світі інформація є найціннішим глобальним ресурсом. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація постійно ускладнюється, змінюється якісно, зростає кількість її джерел і споживачів. Водночас зростає уразливість сучасного інформаційного суспільства від недостовірної (а іноді й шкідливої) інформації, її несвоєчасного надходження, промислового шпигунства, комп'ютерної злочинності, а тому інформація має бути надійно захищена.

Актуальність дослідження. Поняття «інформаційна безпека» історично використовувалось порівняно давно (згідно даних по перших

знайдених публікаціях за тематикою починаючи з 60-тих років минулого сторіччя) [1]. З появою терміну «кібербезпека» між термінами «інформаційна безпека» та «кібербезпека» розпочалась певна конкуренція, сфера вживання цих термінів трактувалась різним чином, різні варіанти трактувань наведено в [1, 2]. В українському законодавстві сучасний зміст терміну «інформаційна безпека» наведено в проекті Закона України «Про внесення змін до законів України щодо інформаційної безпеки» [3] від 26.11.2018, тоді як поняття «кібербезпека» було розкрито раніше, в [4]. У зв'язку із великою кількістю визначень досі немає єдиної думки в точному розумінні відмінностей між поняттям «кібербезпека» та «інформаційна безпека» і суміжними термінами. Також актуальним залишається аналіз тенденцій популярності термінів: «інформаційний простір», «інформаційна безпека», «інформаційна загроза» та «інформаційний ризик».

Актуальність та новизна. В даній роботі проаналізовано різницю в семантиці термінів «інформаційна безпека» та «кібербезпека», з точки зору вітчизняного законодавства та зарубіжного практичного досвіду. А також зібрано та проаналізовано відомості про кількість використання та популярності терміну: «інформаційна безпека», та споріднених термінів «інформаційний простір», «інформаційний ризик», «інформаційна загроза» у публікаціях різних напрямів за період з 80-их років минулого сторіччя дотепер, які знаходяться в онлайн доступі, через використання провідних веб-сервісів. Це дає змогу встановити перспективи використання даних термінів науковим міжнародним суспільством.

Метою даної роботи є дослідження категорії «загроза», вирішення термінологічної проблеми у сфері інформаційної безпеки та встановлення чіткого розділення між кібернетичною сферою. 1

Об'єкт дослідження – використання визначеної термінології у публікаціях різних напрямів та нормативно-правових документах.

Предметом дослідження є контекст, в якому використовуються визначені терміни та динаміка популярності їх вживання.

Методами дослідження є: інтелектуальний аналіз тексту (Text Mining), розвідковий аналіз, порівняльний аналіз, RS-аналіз.

Огляд літератури. В ході написання курсової роботи були використані літературні джерела наступних авторів: Жуков А.С., Попов В.Б., Саврасенко А.А., Романенко В.В.

Структура роботи складається з вступу, основної частини, висновків та пропозицій, списку використаних джерел та додатків.

ДОДАТОК К

ЗРАЗКИ ОФОРМЛЕННЯ БІБЛІОГРАФІЧНИХ ОПИСІВ У СПИСКУ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мінухін С. В. Кавун С. В. Знахур С.В Комп’ютерні мережі. Навчальний посібник Харків, ХНЕУ, 2008. – 210с.
2. О.Д Азаров, С.М. Захарченко, О.В. Кадук, М.М. Орлова, В.П. Тарасенко Комп'ютерні мережі. - Підручник -Вінниця, ВНТУ, 2020.−378с.
3. Вершина А.И. Модель отримання знань / А.И. Вершина, Г.Г. Киричек // Тиждень науки: наук.-техн. конф., 19-23 квіт. 2010 р.: тези доп. – Запоріжжя: ЗНТУ, 2010. – Т. 2. – С.115–116.
4. Біленчук П.Д. Комп’ютерна злочинність / П.Д. Біленчук, Б.В. Романюк, В.С. Цимбалюк та ін. – К. : Атіка, 2002. – 240 с.
5. Мосіяшенко В.А. Мережі [Текст] : навч. посіб. / В. А. Мосіяшенко. — Суми : Унів. кн., 2005. — 174 с.—ISBN 966-680-198-1.
6. Лєпа Є.В. Системи підтримки прийняття рішень. Частина 1 / Є.В. Лєпа, Є.К. Міхеєв, В.В. Крініцин. // Навчальний пособник.– Херсон, 2006. – 324 с.
7. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання [Текст] : (ГОСТ 7.1—2003, IDT) : ДСТУ ГОСТ 7.1:2006. — Чинний з 2007—07—01. — К. : Держспоживстандарт України, 2007. — 47 с. ; 29 см. — (Система стандартів з інформації, бібліотечної та видавничої справи) (Національний стандарт України).

ДОДАТОК Л

Приклад заяви на затвердження теми курсової роботи

Завідувачу кафедри інженерії
програмного забезпечення та кібербезпеки
д.т.н., проф. Криворучко О.В.
Студента ФІТ 3-11 гр.
спеціальності 125 «Кібербезпеки»
Баранова Олександра Сергійовича

ЗАЯВА

Прошу затвердити тему курсової роботи «Методи і способи протидії від витоку інформації по технічним каналам» з дисципліни «Безпека інформаційних систем та мереж» та призначити керівником курсової роботи Савченко Т.В.

«_____»_____ _____