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

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

до виконання курсової роботи
з дисципліни «Захист інформації в інформаційно-комунікаційних системах»
для студентів спеціальності 125 Кібербезпека та захист інформації
освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем

Київ – 2025

Методичні рекомендації до виконання курсової роботи з дисципліни «Захист інформації в інформаційно-комунікаційних системах» для студентів спеціальності 125 Кібербезпека та захист інформації, освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем / Укладачі: Костюк Ю.В., Складанний П.М, Рзаєва С.Л. Київ: КСУБГ, 2025. 70 с.

Методичні рекомендації містять загальні положення про організацію підготовки курсової роботи бакалавра спеціальності 125 Кібербезпека та захист інформації, вимоги до її структурних елементів, виконання та оформлення. Описується порядок та процедура захисту. У додатках наведено зразки документів, що використовуються при підготовці курсової роботи бакалавра.

Рекомендовано Вченою радою Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка (протокол № 2 від 19 лютого 2025 р.)

ЗМІСТ

ВСТУП

Курсова робота відіграє значну роль у розвитку навичок самостійної творчої роботи студента, сприяє поглибленню і узагальненню знань, одержаних студентом, застосуванню цих знань у практичній діяльності. У процесі роботи над курсовою студент повинен показати уміння працювати з літературними джерелами, аналізувати та представляти отримані в ході дослідження результати, робити узагальнення та формулювати висновки.

Методичні рекомендації до виконання курсової роботи з дисципліни «Захист інформації в інформаційно-комунікаційних системах» є нормативним документом Київського столичного університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка для здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека та захист інформації, освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем. Методичні рекомендації укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

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.

Захист курсових робіт відбувається згідно затвердженого графіку. Типова структура курсової роботи має бути такою: титульний аркуш, план-проспект, анотація, зміст, перелік умовних позначень (при необхідності), вступ, 4-5 розділів, що розкривають зміст проблеми та описують результати теоретичного дослідження і практичного завдання, висновки та пропозиції, список використаних джерел, додатки. Робота повинна бути зброшурована, тобто аркуші повинні бути скріплені. Сторінки обов’язково нумеруються.

ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. МЕТА ТА ЗАВДАННЯ КУРСОВОЇ РОБОТИ

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.

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.

Методичні рекомендації висувають загальні вимоги до організації та проведення курсової роботи, тематики, змісту та обсягу, порядку розробки та захисту курсових робіт (КР) відповідно до навчального плану спеціальності 125 Кібербезпека та захист інформації, освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем для здобувачів освітнього рівня першого (бакалаврського) з дисципліни «Захист інформації в інформаційно-комунікаційних системах».

Виконання курсової роботи з дисципліни «Захист інформації в інформаційно-комунікаційних системах» та її захист є формою контролю рівня знань студентів за вивченням даної навчальної дисципліни.

Мета курсової роботи:

- закріпити, поглибити та узагальнити знання, здобуті студентами під час вивчення дисципліни «Захист інформації в інформаційно-комунікаційних системах», з особливим акцентом на спеціальну підготовку в галузі безпеки інформаційних та комунікаційних систем;
- отримання знань і навичок аналізу загроз і заходів щодо їх запобігання програмно-апаратними засобами захисту інформації, а також вбудованими механізмами захисту загальносистемного програмного забезпечення;
- здійснити моніторинг та прогнозування комп'ютерних зловживань та аномалій;
- протидіяти несанкціонованим спробам проникнення в інформаційні системи;
- забезпечити відновлення нормального функціонування інформаційно-комунікаційної системи (ІКС) після реалізації загроз, кібератак, збоїв та відмов різних видів та походження;
- розробити та впровадити комплекс заходів (правила, процедури, практичні прийоми тощо) для управління кібербезпекою;
- виконати спеціальні дослідження технічних і програмно-апаратних засобів захисту інформації та інформаційних систем;

- застосувати криптографічні методи захисту інформаційних та комунікаційних ресурсів;
- використовувати програмні та програмно-апаратні комплекси для захисту інформаційних ресурсів;
- впроваджувати та забезпечувати функціонування комплексних систем захисту;
- забезпечити впровадження та дотримання політики безпеки.

Завдання до курсової роботи передбачає:

✓ Здійснювати моніторинг та прогнозування комп'ютерних зловживань і аномалій, протидіяти несанкціонованим спробам проникнення в інформаційні системи. Відновлювати штатне функціонування інформаційно-комунікаційної системи після реалізації загроз, кібератак, збоїв та відмов різних типів і походження. Розробити комплекс заходів (правила, процедури, практичні прийоми тощо) для ефективного управління кібербезпекою;

✓ Виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту інформації та інформаційних систем, застосовувати криптографічні методи для захисту інформаційних і комунікаційних ресурсів, використовувати програмні та програмно-апаратні комплекси для захисту інформаційних ресурсів. Впроваджувати та забезпечувати функціонування комплексних систем захисту інформації, забезпечувати впровадження та дотримання політики безпеки;

✓ Розв'язувати задачі захисту інформації, що обробляється в інформаційно-комунікаційній системі (ІКС), з використанням сучасних методів і засобів криптографічного захисту. Визначати відомості, що належать до різних видів конфіденційної інформації, організовувати допуск і доступ персоналу до конфіденційних даних згідно з політикою інформаційної та/або кібербезпеки;

✓ Демонструвати знання та розуміння основ побудови комп'ютерних мереж, описувати принципи й методи організації мережевих комунікацій. Демонструвати знання в організації баз даних та розробляти проєкти баз даних інформаційних систем, використовуючи сучасні методи та моделі інформаційної та кібербезпеки;

✓ Проявляти знання в технологіях проєктування комп'ютерних систем захисту інформації, а також діагностиці та експлуатації комп'ютерних систем захисту. На практиці застосовувати засоби автоматичного контролю та діагностування для забезпечення належного рівня безпеки інформаційних систем.

Цілями виконання курсової роботи 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 ІКС, а саме на оцінку ефективності програмних і апаратних рівнів існуючої системи захисту ІКС із застосуванням спеціалізованих інструментаріїв і методів.

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

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 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 курсової роботи (КР) повинне забезпечувати творчу діяльність студента та самостійне розв’язання окремих технічних завдань. Вміст і структура КР мають враховувати специфіку напряму підготовки та вимоги освітньої програми.

Тематика КР тісно пов'язана з майбутньою спеціальністю студентів та присвячена важливим аспектам захисту інформаційно-комунікаційних систем. Для виконання КР пропонується використання сучасних інформаційних технологій, таких як інструменти навантажувального тестування та моніторингу розподілених ресурсів, хмарні та мобільні технології, технології віртуалізації та розпізнавання образів, а також методи 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 інформаційно-комунікаційних ресурсів. Також застосовуються статистичні методи дослідження, математичне та імітаційне моделювання.

Зміст КР визначається завданням, яке видається викладачем на консультації кожному студенту. КР охоплює декілька послідовних етапів, які зазвичай включають аналіз предметної області, постановку задачі, розробку індивідуального технічного завдання, вибір форми подання задачі, розробку математичної моделі об'єкта дослідження, вибір оптимального алгоритму реалізації задачі, розробку сценарію навантаження на об'єкт дослідження, проведення досліджень роботи програми та формулювання обґрунтованих висновків щодо отриманих результатів.

З урахуванням викладеного тематика курсової роботи 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, проєктних 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 курсова робота.

За трудомісткістю КР повинна відповідати терміну, який відведений на курсову роботу навчальним планом.

Виконання курсової роботи з однієї теми кількома студентами однієї групи не припустиме.

1.3. Приклади тем на курсову роботу

1. Захист інформаційно-комунікаційної системи банківського підприємства від витоків інформації через соціальну інженерію та фішинг-атаки.
2. Аналіз ризиків витоку інформації інформаційно-комунікаційної системи компанії з відеоспостереження.
3. Розробка системи моніторингу для виявлення можливих витоків інформації в інформаційно-комунікаційній системі лізингового підприємства.
4. Оцінка ефективності існуючих засобів захисту інформації від витоків у корпоративній мережі навчального закладу.
5. Впровадження політики безпеки для захисту інформації від витоків через мобільні пристрої.
6. Розробка базової системи контролю доступу для запобігання витокам інформації невеликих підприємств.

7. Оцінка ризиків витоку інформації через мережевий трафік і розробка рекомендацій для покращення захисту.

8. Впровадження основних засобів захисту для запобігання витокам інформації в системах з хмарними ресурсами.

9. Розробка методів для управління ризиками витоку інформації в організаціях, що використовують інформаційно-комунікаційні системи.

10. Розробка програмного забезпечення для виявлення шкідливих програм в інформаційно-комунікаційній системі компанії з технічної підтримки.

11. Розробка програмного забезпечення для тестування антивірусних програм в інформаційно-комунікаційній системі IT-компанії.

12. Розробка програмного забезпечення для перевірки захищеності операційної системи в інформаційно-комунікаційній системі промислового підприємства.

13. Розробка системи захищеного резервного копіювання файлів з використанням RAID-масивів в інформаційно-комунікаційній системі наукового підприємства.

14. Захист інформації при використанні електронної пошти в інформаційно-комунікаційній системі державного підприємства.

15. Комплексний підхід до забезпечення захисту конфіденційної інформації логістичної компанії.

16. Організація захисту персональних даних в інформаційно-комунікаційній системі туристичного підприємства.

17. Організація протидії загрозам безпеки інформації в інформаційно-комунікаційній системі підприємства.

18. Побудова типової моделі загроз безпеки інформації в інформаційно-комунікаційній системі виробничого підприємства.

19. Розробка комплексу заходів щодо збереження конфіденційної інформації в інформаційно-комунікаційній системі.

20. Розробка системи захисту комерційної інформації в інформаційно-комунікаційній системі охоронного агентства.

21. Розробка заходів з технічного захисту конфіденційної інформації в інформаційно-комунікаційній системі фінансового підприємства.

22. Розробка політики безпеки для інформаційно-комунікаційної системи міжнародної торговельної компанії.

23. Розробка системи захисту інформації охоронного підприємства на основі інформаційно-комунікаційних систем.

24. Захист комерційної таємниці в інформаційно-комунікаційній системі наукового підприємства.

25. Розробка комплексної системи інженерно-технічного захисту інформації в інформаційно-комунікаційній системі котеджного містечка.

26. Методи і способи протидії витоку інформації по технічним каналам в інформаційно-комунікаційній системі консалтингової компанії.

27. Основні положення і принципи побудови технічного захисту інформації в інформаційно-комунікаційній системі.

28. Розробка рекомендацій щодо вибору технічних засобів системи контролю і управління доступом для захисту інформації в інформаційно-комунікаційній системі державного сервісного підприємства.

29. Розробка методики захисту персональних даних в інформаційно-комунікаційній системі підприємства з медичних послуг.

30. Організаційний захист об'єктів інформаційно-комунікаційної системи торговельного підприємства.

31. Програмно-технічні засоби і методи забезпечення інформаційної безпеки в інформаційно-комунікаційній системі провайдера систем управління доступом.

32. Шляхи вирішення проблем захисту інформації в інформаційно-комунікаційній мережі приватного підприємства.

33. Захист інформації в інформаційно-комунікаційних мережах і хмарних системах науково-дослідної компанії.

34. Безпека програмного забезпечення і мобільних додатків в інформаційно-комунікаційній системі консалтингової компанії.

35. Розробка системи аутентифікації користувачів в інформаційно-комунікаційній системі науково-дослідної лабораторії.

36. Захист комп’ютерної мережі та інформаційно-комунікаційної систем на підприємстві готельного господарства.

37. Сервіси безпеки та механізми її порушень в інформаційно-комунікаційній системі логістичної компанії.

38. Дослідження засобів захисту операційних систем в інформаційно-комунікаційній системі туристичного агентства

39. Захист операційних систем і забезпечення безпеки баз даних в інформаційно-комунікаційній системі готельного комплексу.

40. Аналіз ризику безпеки інформаційно-комунікаційної системи комерційного підприємства.

41. Опис стану оформлення та надання послуг електронного цифрового підпису в інформаційно-комунікаційній системі юридичної компанії.

42. Організаційні заходи по відновленню працездатності інформаційно-комунікаційної системи у випадку виникнення нештатних ситуацій.

43. Організаційні та технічні заходи по резервуванню критично важливої інформації в інформаційно-комунікаційній системі логістичного підприємства.

44. Прогнозування можливих загроз і аналіз пов’язаного з ними ризику для інформаційно-комунікаційної системи енергетичного підприємства.

45. Прийняття принципових рішень в галузі безпеки на основі поточного стану інформаційно-комунікаційної системи.

46. Розробка системи захисту інформації в інформаційно-комунікаційній системі міжнародного підприємства.

47. Методи моделювання системи захисту інформації в інформаційно-комунікаційній системі компанії з технічної підтримки.

48. Опис сучасних загроз для інформації при створенні системи захисту інформації в інформаційно-комунікаційній системі компанії з управління активами.

49. Захист інформації в інформаційно-комунікаційній системі підприємства від витоку по радіоканалу.

50. Захист інформації в інформаційно-комунікаційній системі підприємства від витоку по каналам комунікацій.

51. Захист інформації в інформаційно-комунікаційній системі компанії з систем відеоспостереження від витоку по оптичному каналу.

52. Захист інформації в інформаційно-комунікаційній системі підприємства від витоку по бездротовим каналам зв’язку.

53. Захист інформації в інформаційно-комунікаційній системі підприємства від витоку по побічному електромагнітному випромінюванню.

54. Захист інформації в інформаційно-комунікаційній системі підприємства від витоку по акустичному каналу.

55. Захист інформації в інформаційно-комунікаційній системі підприємства від витоку по інфрачервоному каналу.

56. Захист інформації при проведенні конфіденційних нарад в інформаційно-комунікаційній системі фармацевтичної компанії.

57. Інженерно-технічні системи захисту інформації в інформаційно-комунікаційній системі виробничого підприємства.

58. Програмно-апаратні системи захисту інформації в інформаційно-комунікаційній системі аутсорсингової компанії.

59. Пошук засобів негласного отримання інформації як елемент комплексного захисту інформації в інформаційно-комунікаційній системі транспортної компанії.

60. Побудова інформаційної моделі системи управління захистом інформації в інформаційно-комунікаційній системі банківської установи.

61. Порядок проведення експертизи системи захисту інформації в інформаційно-комунікаційній системі компанії з технічної підтримки.

62. Розробка системи моніторингу та аналізу безпеки мережевого трафіку в корпоративній інформаційно-комунікаційній системі.

63. Впровадження технологій шифрування для захисту конфіденційної інформації під час передачі по каналах зв’язку в інформаційно-комунікаційній системі державного підприємства.

64. Розробка методів захисту від атак типу "людина посередині" (MITM) в корпоративних інформаційно-комунікаційних мережах.

65. Аналіз та оцінка ефективності системи управління інформаційною безпекою (СУІБ) в корпоративному середовищі.

66. Розробка і впровадження системи захисту від кібератак в інформаційно-комунікаційній системі підприємства сфери послуг.

67. Оцінка ефективності методів шифрування для захисту даних в інформаційно-комунікаційній системі енергетичного підприємства на базі хмарних технологій.

68. Розробка стратегії захисту інформації в корпоративних мобільних додатках та їх інтеграція в існуючі інформаційно-комунікаційні системи підприємства.

69. Аналіз і впровадження системи виявлення та запобігання вторгнень (IDS/IPS) в інформаційно-комунікаційну систему логістичного підприємства.

70. Розробка політики безпеки для захисту даних в інформаційно-комунікаційній системі фінансового підприємства з використанням технологій Blockchain.

71. Забезпечення захисту інформації в інформаційно-комунікаційній системі ІТ-компанії за допомогою технологій кіберзахисту та хостової безпеки.

72. Оцінка і вдосконалення механізмів автентифікації та авторизації в інформаційно-комунікаційній системі енергетичної компанії.

73. Моделювання загроз і аналіз ризиків для інформаційно-комунікаційної системи компанії з урахуванням сучасних кібератак.

74. Розробка і впровадження стратегій резервного копіювання та відновлення даних для інформаційно-комунікаційної системи компанії з управління активами.

75. Захист інформації в інформаційно-комунікаційній системі ІТ-компанії від атаки типу «відмова в обслуговуванні» (DoS/DDoS).

76. Оцінка та вдосконалення систем криптографічного захисту даних в інформаційно-комунікаційній системі з виробництва мережевого обладнання.

77. Розробка та реалізація заходів з фізичного захисту інформаційних та комунікаційних систем в корпоративному середовищі.

78. Інтеграція і моніторинг засобів захисту інформації в багатокористувацьких інформаційно-комунікаційних систем та їх ефективність.

79. Розробка політики безпеки для захисту даних в інформаційно-комунікаційній системі з використанням технологій Blockchain.

80. Забезпечення захисту інформації в розподілених інформаційно-комунікаційних системах за допомогою технологій кіберзахисту та хостової безпеки.

81. Оцінка і вдосконалення механізмів автентифікації та авторизації в інформаційно-комунікаційній системі страхового підприємства.

82. Моделювання загроз і аналіз ризиків для інформаційно-комунікаційної системи з урахуванням сучасних кібератак.

83. Розробка і впровадження стратегій резервного копіювання та відновлення даних для інформаційно-комунікаційної системи туристичного підприємства.

84. Розробка та реалізація заходів з фізичного захисту інформаційних та комунікаційних систем в корпоративному середовищі консалтингової компанії.

85. Розробка і впровадження системи моніторингу витоків інформації в інформаційно-комунікаційній системі дослідної лабораторії.

86. Аналіз і впровадження механізмів захисту від витоків конфіденційної інформації через електронну пошту в інформаційно-комунікаційній системі охоронної компанії.

87. Розробка системи контролю та запобігання витокам інформації в хмарних середовищах компанії з систем відеоспостереження.

88. Оцінка ризиків витоку інформації через бездротові комунікаційні канали в інформаційно-комунікаційній системі холдингової компанії.

89. Захист інформаційно-комунікаційної системи від витоків даних через фізичні канали, такі як USB-порти та інші периферійні пристрої.

90. Розробка і впровадження технологій для захисту від витоків інформації в інтегрованій інформаційно-комунікаційній системі аутсортингової компанії.

91. Аналіз і впровадження заходів для запобігання витоку інформації в результаті неправильного використання програмного забезпечення IT-компанії.

92. Оцінка ефективності методів шифрування для запобігання витоку інформації в інформаційно-комунікаційній системі логістичної компанії.

93. Розробка і реалізація політик контролю доступу для захисту інформації від витоку в інформаційно-комунікаційній системі виробничого підприємства.

94. Електронний цифровий підпис як засіб захисту документів в інформаційно-комунікаційній системі державного підприємства.

95. Акустичні канали витоку інформації: методи захисту та засоби протидії в інформаційно-комунікаційній системі.

96. Захист серверних приміщень в інформаційно-комунікаційній системі: технічні та організаційні заходи.

97. Концепція безпеки при створенні системи фізичного захисту об’єктів інформаційної діяльності.

98. Оптичні засоби здобуття інформації: загрози для інформаційно-комунікаційної системи та методи захисту.

99. Аналіз ризиків та засоби протидії перехопленню аудіоінформації в інформаційно-комунікаційній системі компанії з технічної підтримки.

100. Методи технічного контролю ефективності заходів захисту

інформації в інформаційно-комунікаційній системі комерційного підприємства.

1.4. Порядок виконання

Вибір теми студентом здійснюється на початку семестру. Студент обговорює тему курсової роботи з викладачем, складає план роботи та список літератури з обраної теми. Вивчення літератури необхідно розпочати з нормативно-правових актів України та нормативних документів системи технічного захисту інформації (ТЗІ), а потім перейти до вивчення наявної експлуатаційно-технічної документації та більш спеціальних досліджень, наприклад наукових статей. У процесі виконання роботи студент підтримує зв'язок з викладачем, звертаючись до нього за консультацією по мірі виникнення питань або ускладнень.

Складання розширеного плану роботи студентом здійснюється протягом першої половини семестру. Роль викладача полягає в уточненні плану роботи та списку літератури за темою, обговоренні предмету, об'єкту, мети та завдань дослідження, повноти та достатності викладення теми, сприянні творчим пошукам за темою роботи, а також у підготовці студента до захисту курсової роботи.

Оформлюючи роботу, студент спочатку складає її електронний (чорновий) варіант та представляє його викладачу. Після перевірки, враховуючи зауваження та вказівки, студент доопрацьовує роботу.

Студент подає роботу для перевірки, оформлює роботу у відповідності до вимог. Після цього робота друкується та пред'являється викладачу не пізніше ніж за тиждень до дати захисту.

На захист студент повинен підготувати доповідь та презентацію по результатам проведеної роботи. Студент розробляє презентацію роботи за допомогою засобів «Microsoft Office PowerPoint» тривалістю 3-5 хвилин. Захист курсової роботи здійснюється згідно графіку захисту курсових робіт.

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 тиждень
2.	Необхідно провести аналіз предметної області та характеристику об'єкта дослідження. Першим етапом є визначення мети роботи, загальної характеристики об'єкта дослідження та опис його параметрів функціонування (метрик). Слід також провести порівняльний аналіз об'єкта дослідження в контексті його взаємодії з іншими компонентами	3-4 тиждень

	обчислювальної системи. Результати цього етапу повинні бути оформлені в електронному варіанті 1-го розділу.	
4	Другим етапом є планування програмно-технічного середовища та розробка основних вимог до розв'язання поставленої задачі. Необхідно визначити порядок проведення дослідження, можливий ступінь навантаження, а також провести аналіз інструментів моніторингу об'єкта дослідження та середовища оточення, порівняти їх переваги та недоліки. Важливо також визначити потребу в розробці програмного коду та скриптів для досягнення поставленої мети. Результати цього етапу слід подати в електронному варіанті 2-го розділу.	5-7 тиждень
5	Третій етап передбачає безпосереднє дослідження порушення доступності ресурсу. Для цього потрібно підготувати об'єкт дослідження та необхідні програмні засоби, встановити операційну систему, віртуальні машини, інструменти навантаження та моніторингу, а також отримати результати виконання дослідження. Ці результати повинні бути оформлені в електронному варіанті 3-го розділу.	7-9 тиждень
6	На четвертому етапі необхідно провести аналіз та інтерпретацію отриманих результатів дослідження. Це включає розрахунок описової статистики, застосування методів статистичного аналізу та моделювання систем. Також потрібно створити математичну модель порушення доступності та визначити межі доступності функціонування об'єкта дослідження. Результати цього етапу повинні бути представлені в електронному варіанті 4-го розділу.	10-13 тиждень
10	Оформлення пояснювальної записки	14 тиждень
11	Завершальне оформлення пояснювальної записки до курсової роботи. Захист курсової роботи	15 тиждень

1.5. Складові частини

Організаційно процес курсового проєктування складається з наступних етапів:

- підготовчого, на якому студент отримує тему, узгоджує з керівником об'єкт проєктування, 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.

1.6. Захист курсових робіт

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

Захист КР проводиться у формі співбесіди зі з'ясуванням всіх питань, що виникли у керівника під час перевірки курсової роботи та під час захисту.

Оцінка за курсову роботу виставляться за державною шкалою.

На оцінку за КР впливають:

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

На доповідь дається 5 хвилин. Після закінчення доповіді викладач може задавати питання, призначення яких – уточнити рівень кваліфікації і ступень самостійності доповідача. За результатами захисту визначається оцінка, 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.

2. СТРУКТУРА КУРСОВОЇ РОБОТИ

2.1. 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 «Захист інформації в інформаційно-комунікаційній системі» розпочинається з оформлення 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 28 до 40 сторінок (не рекомендовано обсяг більший за 45 сторінок), причому технічна її частина, у якій викладаються конкретні дані про розробку конкретної КМ, має містити не менш ніж 20 – 25 сторінок тексту з рисунками. Рисунки можуть містити необхідні для пояснень і розрахунків фрагменти загальної моделі мережі.

До записки додаються додатки формату А4 (структурна схема мережі, функціональна схема мережі, тощо) того ж формату.

Бібліографічні описи в переліку посилань 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

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

1. Титульний лист (Додаток А)
2. Індивідуальне завдання на курсовий проєкт за формою (Додаток Б)
3. Анотація (Додаток В)
4. Перелік умовних позначень, одиниць, символів, скорочень і термінів (Додаток Г)
4. Зміст роботи (Додаток Д)

ВСТУП (Додаток Ж)

Вступ повинен розкрити:

актуальність теми, об’єкт, предмет, мета та завдання дослідження. У вступі потрібно добиватися стислості та чіткості розкриття матеріалу.

ОСНОВНА ЧАСТИНА.

Основна теоретична частина курсової роботи – це виклад відомостей про предмет (об’єкт) дослідження, які є необхідними і достатніми для розкриття сутності означеної роботи (опис теорії, заходів, засобів і методів захисту інформації) та її результати.

Текст курсової роботи викладають, поділяючи матеріал на тематичні розділи. Розділи можуть поділятися на підрозділи та пункти, що послідовно розкривають визначені завдання дослідження. Кожен пункт повинен містити закінчену інформацію.

У першому розділі здійснюється детальний опис об'єкта дослідження, що включає аналіз предметної області та визначення мети роботи. Важливо надати загальну характеристику інформаційно-комунікаційної системи, яка є предметом дослідження, описати її основні компоненти та функціональні можливості. Це допоможе чітко сформулювати мету дослідження, яка може полягати в аналізі, покращенні або оцінці механізмів захисту інформації в системі. У цьому ж розділі потрібно детально описати об'єкт дослідження, включаючи сервери, мережеві пристрої та програмне забезпечення, що забезпечує захист інформації.

Другий розділ присвячено проектуванню системи захисту інформації. Тут необхідно розробити план побудови програмно-технічного середовища, що включає вибір програмних і апаратних засобів для реалізації заходів захисту. Описуються основні вимоги до системи захисту, такі як шифрування даних, контроль доступу та інші засоби захисту. У цьому розділі також важливо оцінити параметри функціонування системи, такі як продуктивність, надійність і рівень безпеки. Аналіз інструментів моніторингу системи і середовища оточення включає порівняння їх переваг і недоліків, а також вибір найбільш підходящих засобів. Також слід визначити необхідність написання

програмного коду або скриптів для вдосконалення заходів захисту.

Третій розділ охоплює безпосереднє проведення дослідження. Це передбачає підготовку об'єкта дослідження, включаючи налаштування і конфігурацію системи, встановлення необхідного програмного забезпечення і інструментів для моніторингу. Проводяться експерименти та тести для оцінки ефективності впроваджених заходів захисту, а також оцінюються результати тестувань, виявляються слабкі місця і можливі уразливості.

У четвертому розділі проводиться аналіз і інтерпретація отриманих результатів дослідження. Це включає обробку даних, отриманих в результаті тестувань, проведення розрахунків, статистичного аналізу та моделювання для оцінки ефективності заходів захисту. Розробляється математична модель системи захисту інформації, що описує її поведінку під час можливих атак або спроб порушення захисту. Важливо також визначити межу доступності інформаційних ресурсів та їх захисту від несанкціонованого доступу.

Заключний розділ містить висновки та рекомендації. У висновках підводяться підсумки проведеного дослідження, узагальнюються основні результати і висновки. Рекомендації стосуються покращення системи захисту інформації, включаючи вдосконалення існуючих заходів захисту, впровадження нових технологій і методів для підвищення рівня безпеки. Висновки повинні бути тісно переплетені з основною частиною та вступом, не відрізнятися від них за стилем і змістом. Перехід до них є гармонійним продовженням роботи, що відбиває її результат в стислій формі обсягом на 1-2 сторінки.

Висновки визначають підсумок курсової роботи з виводами щодо досліджуваних питань, містять авторську думку, переваги та проблеми, що розкриваються в дослідженні.

Висновки пишуться стисло з викладом проблем і раціональними та добре обдуманими шляхами їх вирішення з описом очікуваного ефекту від проведених дій, рекомендованих у подальшому для впровадження в практичну діяльність.

Висновки можна розпочинати зі слів «підводячи підсумки», «в результаті викладеної інформації» або «на підставі проведених досліджень». Далі вказуються завдання, які вдалося вирішити в ході виконаної роботи. Також необхідно розповісти, що не вдалося вивчити, дослідити та розкрити, які проблеми при цьому виникали, що гальмувало процес дослідження. Висновки розміщують безпосередньо після викладу тематичних розділів, починаючи з нової сторінки.

Таким чином, основна частина курсової роботи забезпечує комплексний підхід до дослідження і вдосконалення систем захисту інформації, дозволяючи детально розглянути всі аспекти, що впливають на безпеку інформаційно-комунікаційних систем.

Список використаних джерел (приклад у Додатку К). Список використаних джерел має містити не менше 15-ти назв наукової та

періодичної літератури, яка була використана під час виконання роботи, а саме: книг, підручників, навчальних посібників, монографій, нормативних документів, статей у періодичних виданнях, інтернет-сайтів тощо. Перелік записується в алфавітному порядку або в порядку згадування в роботі.

Рекомендується використовувати джерела, які опубліковані за останні 5-10 років. Посилання на літературні джерела подають у квадратних дужках із зазначенням номера джерела, наприклад: «…аналіз властивостей пристроїв [10] показав…», а при дослівному цитуванні вказується також номер сторінки, наприклад: [10, с.48].

Додатки. Додатки вміщують матеріал, який оформлюється окремими документами та є необхідним для повноти курсової роботи: експертні висновки, схеми, креслення тощо. Кожен додаток повинен починатися з нового аркуша і мати заголовок. Заголовок друкують вгорі малими літерами з першої великої симетрично до тексту сторінки.

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

2.2. Вимоги до змісту розділів, оформлення та обсягу

До *пояснювальної записки (ПЗ*) необхідно включати матеріал, який безпосередньо відноситься до конкретного об’єкта захисту. Не рекомендується робити великі реферативні огляди. При необхідності можна робити посилання на відповідну літературу. Основний зміст записки – це обґрунтування прийнятих рішень та модель захисту, 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. а також загальний огляд об'єкта і його значення для захисту інформації. а також загальний огляд об'єкта і його значення для захисту інформації. 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.

В процесі розробки системи захисту інформації на об'єкті захисту повинні бути розроблені:

- **Програмні рішення:**
  - *Системи контролю доступу*: розробка програмного забезпечення для ефективного управління доступом до інформаційних ресурсів, включаючи аутентифікацію та авторизацію користувачів.
  - *Механізми шифрування даних:* впровадження алгоритмів шифрування для забезпечення захисту даних як при зберіганні, так і під час передачі.
  - *Антивірусні та антишпигунські програми:* розробка або інтеграція програм для виявлення і нейтралізації шкідливого програмного забезпечення та шпигунських агентів.
  - *Системи виявлення та запобігання вторгнень (IDS/IPS):* налаштування програмних засобів для моніторингу мережевого трафіку та виявлення підозрілої активності.
  - *Політики і процедури інформаційної безпеки:* створення та впровадження політик, процедур та стандартів для управління інформаційною безпекою, включаючи управління інцидентами та реагування на них.
- **Апаратні рішення:**
  - *Апаратні засоби шифрування:* вибір і впровадження пристроїв для апаратного шифрування даних, що забезпечують високий рівень захисту від несанкціонованого доступу.

- ✓ *Системи фізичного контролю доступу:* інсталяція фізичних систем контролю доступу, таких як біометричні сканери, картки з чіпами та електронні замки.
- ✓ *Обладнання для моніторингу:* установка датчиків і камер відеоспостереження для контроля фізичного доступу і моніторингу об'єктів захисту.
- ✓ *Засоби захисту від електромагнітних витоків:* впровадження екранів і фільтрів для захисту від витоків інформації через електромагнітні поля.

❖ **Моделювання загроз і ризиків:**

- ✓ *Моделі загроз:* розробка моделей загроз для визначення можливих шляхів витоку інформації через акустичні, оптичні, віброакустичні та електромагнітні канали.
- ✓ *Оцінка ризиків:* моделювання ризиків для оцінки ймовірності і наслідків потенційних загроз та їх впливу на інформаційні *системи.*
- ✓ *Симуляції атак:* проведення тестових атак і симуляцій для перевірки ефективності існуючих заходів захисту і виявлення можливих вразливостей.
- ✓ *Моделі порушень:* розробка моделей для розуміння можливих сценаріїв порушення безпеки, що допоможе виявити потенційні слабкі місця системи захисту.

Ці заходи дозволять створити всебічну і ефективну систему захисту інформації, що охоплює всі можливі аспекти загроз і вразливостей, забезпечуючи комплексний захист інформаційних ресурсів на об'єкті.

Курсова робота повинна містити графічну частину і записку пояснення.

Графічна частина

Графічна частина пояснювальної записки різноманітні графічні елементи, які допомагають візуалізувати інформацію, аналізувати дані і підтримувати текстову частину роботи. Кожна схема виконується на окремому листі формату А4.

Розділ 1. Струкуризація інформації, що захищається

У цьому розділі важливо визначити різні категорії інформації, що потребує захисту, включаючи конфіденційну, секретну та чутливу інформацію. Необхідно розробити класифікацію даних на основі їх важливості та впливу на організацію у випадку витоку або порушення конфіденційності. Слід описати моделі загроз, що пов’язані з кожною категорією інформації, а також визначити, які політики інформаційної безпеки необхідні для забезпечення належного захисту. Цей розділ також повинен включати специфікацію вимог до програмно-апаратного захисту інформації, таких як системи контролю доступу, шифрування даних і засоби для захисту від вірусів.

Розділ 2. Аналіз та моделювання можливих каналів витоку інформації на обраному об'єкті захисту

Цей розділ повинен охоплювати детальний аналіз потенційних каналів витоку інформації, включаючи акустичні, оптичні, електромагнітні та віброакустичні канали. Потрібно описати особливості технічних каналів витоку і несанкціонованого доступу до інформації. Необхідно моделювати можливі сценарії витоку інформації та оцінити ризики, пов’язані з кожним каналом. Важливо також розглянути моделі порушень, щоб передбачити різні способи, якими зловмисники можуть скористатися для отримання доступу до конфіденційної інформації. Для цього можуть використовуватися як програмні інструменти для виявлення потенційних загроз, так і апаратні засоби для захисту від витоку інформації.

Розділ 3. Оцінка ступеня загрози інформації, що захищається

У цьому розділі слід провести детальну оцінку загроз для інформації на основі результатів моделювання з попереднього розділу. Оцінка включає визначення ймовірності реалізації кожної загрози і можливих наслідків витоку інформації. Необхідно оцінити ефективність існуючих заходів захисту і визначити їх відповідність до потенційних загроз. Цей розділ має також розглянути потенційний вплив порушення безпеки на організацію, включаючи фінансові, юридичні та репутаційні наслідки. Провести моделювання об’єктів захисту.

Розділ 4. Розробка заходів щодо захисту інформації на об'єкті захисту

На основі аналізу загроз і оцінки ризиків, у цьому розділі слід розробити конкретні заходи захисту інформації. Обрати необхідні методи і засоби блокування каналів витоку інформації. Включити як технічні, так і організаційні заходи. Технічні заходи можуть включати впровадження систем шифрування, програмного забезпечення для захисту від вірусів, міжмережевих екранів (фаєрволів) і систем виявлення вторгнень. Організаційні заходи можуть включати створення політик інформаційної безпеки, проведення навчання персоналу і розробку процедур реагування на інциденти. Необхідно також визначити технічні засоби захисту для запобігання фізичному доступу до критичних систем і даних.

Розділ 5. Схема та вибір розміщення технічних засобів захисту інформації на об'єкті.

Цей розділ присвячений розробці та реалізації схеми розміщення технічних засобів захисту. Важливо вибрати та розмістити апаратні засоби, такі як датчики, системи контролю доступу, обладнання для моніторингу та фільтрації трафіку, у стратегічно важливих точках. Розробка схеми повинна включати розрахунок оптимального розміщення для забезпечення максимальної ефективності захисту при мінімальних витратах. Необхідно також врахувати аспект інтеграції технічних засобів з існуючими

інформаційними системами та їх можливість масштабування в разі необхідності.

У *висновках* (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 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.

3. ПРАКТИЧНА ЧАСТИНА КУРСОВОЇ РОБОТИ

3.1. Загальні відомості

Сучасні інформаційні системи різного призначення, розміру, форми власності можуть мати спільні риси і, навидь, схожу структуру. Наведемо приклад організації (компанії, підприємства) з позиції обробки інформації (наприклад, страхової компанії, виробничого об’єднання, органу державної влади, тощо) (рис. 3.1). Інформація такої організації обробляється з використанням інформаційно-комунікаційної системи, приклад структурної схеми якої наведено.

Структурна схема інформаційно-комунікаційної системи (ІКС) включає джерела інформації, обробні пристрої, системи зберігання даних, комунікаційні канали, інтерфейси користувача та системи захисту інформації. Джерела інформації постачають дані, обробні пристрої їх аналізують, системи зберігання забезпечують зберігання, комунікаційні канали передають дані, а системи захисту забезпечують безпеку і конфіденційність інформації.

Джерела інформації - це пристрої або системи, які генерують або отримують дані, такі як сенсори, користувачі та зовнішні системи. Обробні пристрої, зокрема сервери і комп'ютери, виконують функції обробки даних, управлінські та аналітичні завдання. Системи зберігання даних, включаючи бази даних і файлові системи, забезпечують зберігання і доступність даних.

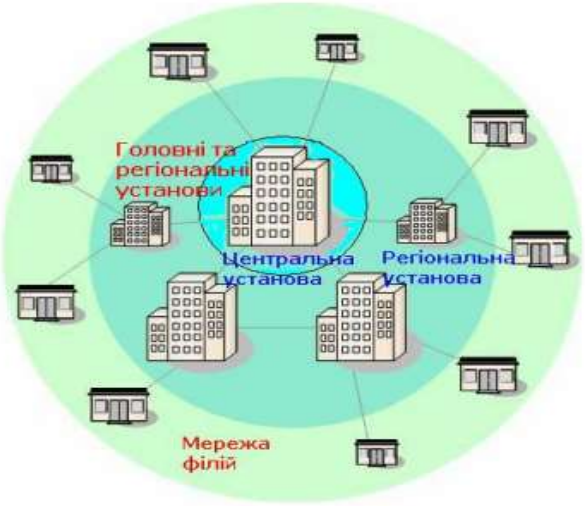


Рис. 3.1. Приклад організації (компанії) з позиції обробки інформації (*Центральна установа забезпечує накопичення та аналітичну обробку інформації, централізовану підтримку служб, а також реалізацію стратегій масштабу організації*)

Комунікаційні канали, такі як локальні мережі і Інтернет, забезпечують передачу даних між джерелами інформації, обробними пристроями і системами зберігання. Керуючі системи відповідають за управління функціонуванням ІКС, включаючи моніторинг, адміністрування і безпеку. Інтерфейси користувача надають засоби для взаємодії користувачів з системою, такі як графічні інтерфейси або веб-додатки. Системи захисту інформації реалізують заходи для забезпечення безпеки даних, включаючи шифрування, автентифікацію та контроль доступу.

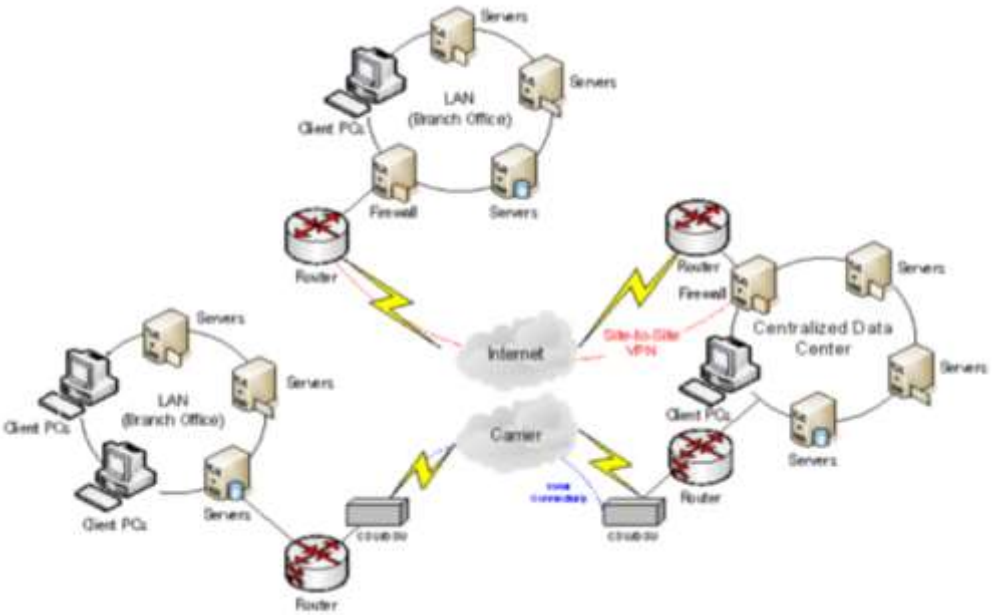


Рис. 3.2. Структурна схема ІКС

Усі ці компоненти взаємодіють між собою, щоб забезпечити ефективну обробку, зберігання і передачу інформації, при цьому дотримуючи вимог безпеки та конфіденційності.

У будь-якій ІКС можна виділити типові рівні, на яких вирішуються задачі, спільні для всіх систем. Як правило, виділяють 4 рівня ІКС (рис. 3.3).

Рис. 3.3. Типові рівні ІКС

Типові рівні ІКС знизу вверх:

- ***Рівень мережі*** – відповідає за взаємодію вузлів ІКС. Елементами ІКС, що відносяться до цього рівня, є модулі, які реалізують стеки протоколів мережевої взаємодії, наприклад, TCP/IP. Також на цьому рівні функціонує специфічна апаратура – мережеве обладнання.
- ***Рівень операційних систем (ОС)*** – відповідає за обслуговування програмного забезпечення, яке реалізує більш високі рівні, і його взаємодію з обладнанням. В якості типових елементів цього рівня можна назвати такі поширені ОС, як Microsoft Windows, Sun Solaris, Linux.
- ***Рівень систем керування базами даних (СКБД)*** – відповідає за зберігання та обробку даних. В якості типових елементів цього рівня можна назвати СКБД Oracle і MS SQL Server. Іноді СКБД є центральним елементом ІС (наприклад, облік товарів на складі), а іноді СКБД функціонує прозоро для користувачів і виконує допоміжні функції, зокрема для зберігання технологічної інформації самої ІС. Так, наприклад, система підтримки. конфіденційного документообігу OPTiMA WorkFlow базується на СКБД MS SQL Server.
- ***Рівень прикладного ПЗ (застосувань)*** - найвищий рівень. Розрізняють прикладний компонент і компонент подання, які є складовими прикладного рівня. Прикладний компонент забезпечує виконання специфічних функцій ІС. Компонент подання відповідає за взаємодію з користувачем і подання даних у необхідній формі. На рівні прикладного ПЗ функціонують, наприклад, офісні застосування, такі як популярні Microsoft Office, Star Office або Open Office, бухгалтерські програми, спеціально розроблені для кожної окремої ІС програмні засоби, що реалізують специфічні для неї функції, і будь-які інші прикладні програми.

У зв’язку з несприятливою криміногенною обстановкою,

недобросовісною конкуренцією та активацією терористичних дій, суспільство змушене зосередитися на проблемах забезпечення безпеки, де інформаційна безпека займає одне з найважливіших місць. Реалізація ефективних систем безпеки вимагає ретельного дослідження можливих технічних каналів витоку інформації та несанкціонованого доступу:

1. **Вивчення можливих каналів витоку:**

   Необхідно детально аналізувати різні канали витоку інформації, включаючи акустичні, оптичні, віброакустичні та електромагнітні. Кожен з цих каналів має свої специфічні параметри та характеристики, які потрібно врахувати для розробки ефективних заходів захисту.

2. **Оцінка параметрів і характеристик витоків:**

   Важливо провести детальне моделювання і аналіз технічних аспектів, які можуть призвести до витоку інформації. Це включає визначення потенційних слабких місць системи, через які можлива несанкціонована передача конфіденційної інформації.

3. **Розробка заходів захисту:**

   На основі проведеного аналізу необхідно розробити та впровадити комплекс заходів для захисту інформації. Це може включати як програмні, так і апаратні рішення, що забезпечують захист від ідентифікованих каналів витоку.

Таким чином, для створення ефективних систем безпеки в інформаційно-комунікаційній системі потрібно детально досліджувати можливі канали витоку інформації та їх параметри, що дозволить забезпечити надійний захист конфіденційних даних і запобігти несанкціонованому доступу.

Одним з напрямків захисту інформації в інформаційно-комунікаційній системі є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу (НСД) і захисту інформації від витоку технічними каналами. Під НСД мається на увазі доступ до інформації, що порушує встановлену в інформаційно-комунікаційній системі (ІКС) політику розмежування доступу. Під технічними каналами розглядаються канали сторонніх електромагнітних випромінювань і наведень (ПЕМІН), акустичні канали, оптичні канали і ін.

Захист від НСД може здійснюватися в різних складових ІКС:

− прикладне і системне ПЗ;

− апаратна частина серверів і робочих станцій;

− комунікаційне устаткування і канали зв'язку;

− периметр інформаційної системи.

Для захисту інформації на рівні прикладного і системного ПЗ використовуються:

− системи розмежування доступу до інформації;

− системи ідентифікації і аутентифікації;

− системи аудиту і моніторингу;

− системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення використовуються:

− апаратні ключі;

− системи сигналізації;

− засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

У комунікаційних системах використовуються наступні засоби мережного захисту інформації:

− міжмережні екрани (Firewall) – для блокування атак із зовнішнього середовища (Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway і Alteon Switched Firewall від компанії Nortel Networks). Вони управляють проходженням мережного трафіка відповідно до правил (policies) безпеки. Як правило, міжмережні екрани встановлюються на вході мережі і розділяють внутрішні (частки) і зовнішні (загального доступу) мережі;

− системи виявлення вторгнень (IDS - Intrusion Detection System) – для виявлення спроб несанкціонованого доступу як ззовні, так і усередині мережі, захисту від атак типу "відмова в обслуговуванні" (Cisco Secure IDS, Intruder Alert і NetProwler від компанії Symantec). Використовуючи спеціальні 12 механізми, системи виявлення вторгнень здатні запобігати шкідливим діям, що дозволяє значно знизити час простою в результаті атаки і витрати на підтримку працездатності мережі;

− засоби створення віртуальних приватних мереж (VPN - Virtual Private Network) – для організації захищених каналів передачі даних через незахищене середовище (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator). Віртуальні приватні мережі забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її динамічного шифрування;

− засоби аналізу захищеності – для аналізу захищеності корпоративної мережі і виявлення можливих каналів реалізації загроз інформації (Symantec Enterprise Security Manager, Symantec NetRecon). Їх застосування дозволяє запобігти можливим атакам на корпоративну мережу, оптимізувати витрати на захист інформації і контролювати поточний стан захищеності мережі.

Для захисту периметра ІКС створюються:

− системи охоронної і пожежної сигналізації;

− системи цифрового відеоспостереження;

− системи контролю і керування доступом (СККД).

Захист інформації від її витоку технічними каналами зв'язку забезпечується наступними засобами і заходами:

− використанням екранованого кабелю іпрокладкою проводів і кабелів в екранованих конструкціях;

− установкою на лініях зв'язку високочастотних фільтрів;

− побудовою екранованих приміщень ("капсул");

− використанням екранованого устаткування; − установкою активних систем зашумлення.

Впровадження систем виявлення і запобігання вторгненням (IDS/IPS) забезпечує моніторинг і захист мережевої інфраструктури:

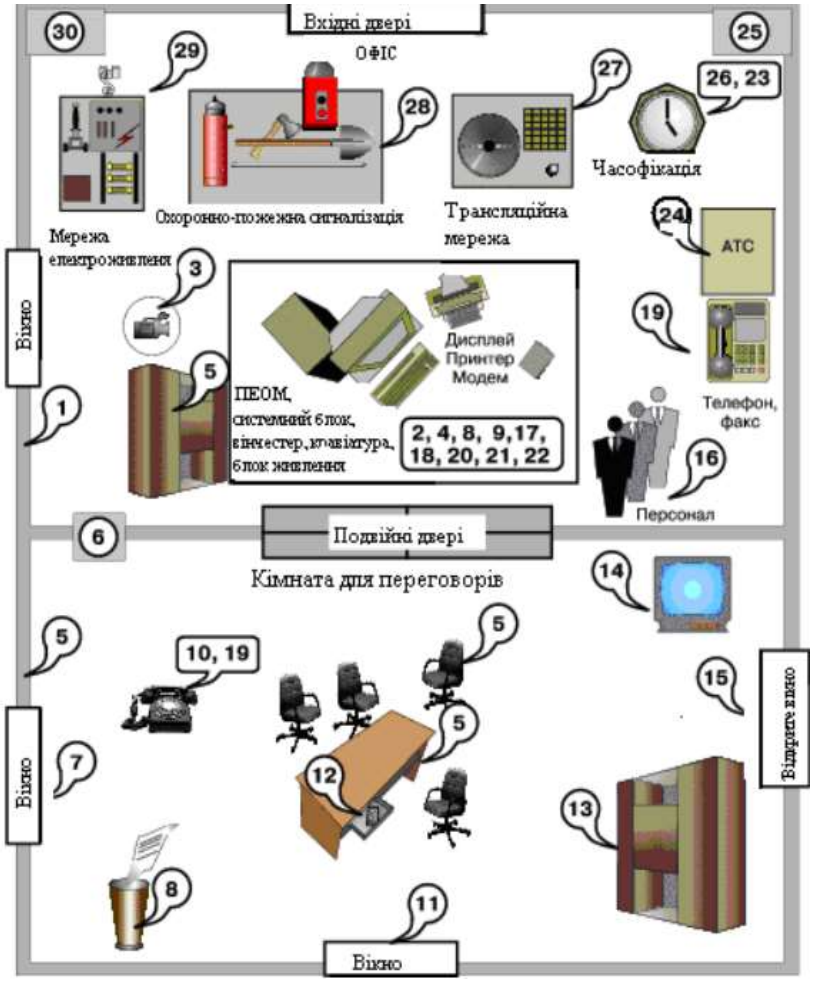
- ✓ ***Системи виявлення вторгнень (IDS)*** — системи, які моніторять мережевий трафік і системні події для виявлення підозрілої або небезпечної активності.
- ✓ ***Системи запобігання вторгненням (IPS)*** — активні системи, які не лише виявляють, але і автоматично блокують або зменшують загрози у реальному часі.

3.2. Просторова і структурна моделі приміщення (наприклад для переговорів)

Захист інформації в інформаційно-комунікаційній системі охоплює організаційні, технічні та правові заходи для запобігання шкоди інтересам власника інформації. Основні об'єкти захисту включають інформацію з обмеженим доступом, технічні засоби обробки та зберігання інформації, а також допоміжні технічні засоби і системи, що не є частиною основних технічних засобів, але розташовані в приміщеннях, де обробляється інформація (рис. 3.4):

У контексті захисту інформації в інформаційно-комунікаційній системі особливо важливо забезпечити конфіденційність, наприклад у приміщеннях, де проводяться переговори. Приміщення для переговорів, де обговорюються питання, що мають конфіденційний характер, стають невід'ємною частиною сучасних організацій. У таких приміщеннях часто відсутні технічні засоби обробки чи передачі інформації, що підкреслює необхідність фізичного та технічного захисту для попередження можливого витоку інформації через просторові та структурні фактори.

В умовах зростання ризиків несанкціонованого доступу до конфіденційної інформації, питання забезпечення безпеки інформації в приміщеннях для переговорів набуває все більшої актуальності. Організація просторової і структурної моделі приміщення є важливою складовою забезпечення інформаційної безпеки в інформаційно-комунікаційній системі. Вибір методів і засобів захисту, що відповідають специфіці приміщення, є ключовим фактором у створенні надійної системи захисту.



1. витік за рахунок структурного звуку в стінах і перекриттях;
2. знімання інформації зі стрічки принтера, погано стертих дискет і т. п.;
3. знімання інформації з використанням відеозакладок;
4. програмно-апаратні закладки в ПЕОМ;
5. радіо-закладки в стінах і меблях;
6. знімання інформації з системи вентиляції;
7. лазерне знімання акустичної інформації з вікон;
8. виробничі й технологічні відходи; 9. комп'ютерні віруси, логічні бомби й т. п.;
10. знімання інформації за рахунок наведень і "нав'язування";
11. дистанційне знімання відео інформації (оптика);
12. знімання акустичної інформації з використанням диктофонів;
13. розкрадання носіїв інформації; 14. високочастотний канал витоку в побутовій техніці;
15. знімання інформації спрямованим мікрофоном;
16. внутрішні канали витоку інформації (через обслуговуючий персонал);
17. несанкціоноване копіювання;
18. витік за рахунок побічного випромінювання термінала;
19. знімання інформації за рахунок використання "телефонного вуха";
20. знімання з клавіатури й принтера акустичним каналом;
21. знімання з дисплея по електромагнітному каналу;
22. візуальне знімання з дисплея й принтера;
23. наведення на лінії комунікацій і сторонні провідники;
24. витік через лінії зв'язку;
25. витік мережею заземлення;
26. витік мережею часофікації;
27. витік трансляційною мережею й гучномовним зв'язком;
28. витік охоронно-пожежною сигналізацією;
29. витік мережею електроживлення;
30. витік мережею опалення, газо- і водопостачання.

Рис. 3.4. Схема каналу витоку і несанкціонованого доступу до інформації в типовому одноповерховому офісі

Метою роботи є розробка та впровадження ефективних заходів захисту конфіденційної інформації в приміщеннях для переговорів, враховуючи особливості їх просторової і структурної моделі. Основні завдання включають:

1. Визначення ключових завдань захисту інформації в приміщеннях для переговорів.
2. Аналіз сучасних методів захисту від витоку інформації через різні канали.

3. Розробка плану заходів щодо забезпечення безпеки інформації в таких приміщеннях.

Для ефективного захисту інформації в приміщеннях для переговорів у межах інформаційно-комунікаційної системи необхідно вирішити такі завдання (рис. 3.5.):

Рис. 3.5.Завдання забезпечення безпеки конфіденційної інформації в кімнаті для переговорів

1. **Захист від акустичного витоку (АК):** розробка і впровадження заходів, що мінімізують можливість перехоплення звукових сигналів, які виникають під час переговорів, у просторі приміщення.
2. **Захист від віброакустичного витоку (ВАК):** застосування методів, що запобігають передаванню звукової інформації через вібрації конструкцій приміщення.
3. **Захист від електроакустичного перетворення (ЕАП):** використання спеціальних технічних засобів, що запобігають витоку інформації через електричні пристрої, які можуть перетворювати акустичні сигнали в електричні.
4. **Захист від високочастотного нав'язування (ВЧН):** забезпечення захисту від можливого впливу високочастотних сигналів, які можуть бути використані для витоку інформації.
5. **Захист від оптичного витоку (ОК):** розробка і впровадження заходів, спрямованих на запобігання перехопленню інформації через оптичні канали.

Для досягнення мети роботи пропонується виконати такі дії:

- ✓ **Аналіз приміщення:** проведення візуального огляду та обстеження приміщення на наявність можливих технічних засобів для перехоплення інформації (закладних пристроїв).
- ✓ **Використання спеціального обладнання:** застосування сучасних технічних засобів для виявлення та нейтралізації загроз перехоплення інформації в інформаційно-комунікаційній системі.
- ✓ **Розробка рекомендацій:** на основі отриманих результатів обстеження сформулювати рекомендації щодо вдосконалення просторової і

структурної моделі приміщення для переговорів з метою підвищення захисту конфіденційної інформації.

В результаті виконання роботи буде розроблена просторово-структурна модель захисту інформації в приміщеннях для переговорів. Вона включатиме комплекс заходів, спрямованих на мінімізацію ризиків витоку конфіденційної інформації через різні канали у межах інформаційно-комунікаційних систем. Ця модель може бути використана як базовий шаблон для захисту інформації в аналогічних приміщеннях інших організацій.

3.3. Моделі загроз та заходи захисту

Усвідомивши основну мету і завдання захисту інформації, можна перейти до розробки моделі загроз для конфіденційної інформації, що мають місце, наприклад, при веденні переговорів (розмов). Моделі загроз доцільно розробляти, узгодивши їх із завданнями захисту.

Моделі загроз та заходи захисту — це структуровані підходи до виявлення потенційних ризиків для інформації та визначення способів їхнього нейтралізування. Моделі загроз описують можливі сценарії атак, джерела загроз, їхні цілі та методи, що використовуються для порушення безпеки. Заходи захисту включають технічні, програмні та організаційні рішення, спрямовані на попередження, виявлення та реагування на ці загрози, забезпечуючи збереження конфіденційності, цілісності та доступності інформації.

Модель загроз для інформації через акустичний канал витоку

Модель загроз для інформації через акустичний канал витоку - це аналіз потенційних загроз, які виникають у результаті прослуховування або запису звукових хвиль, що містять конфіденційну інформацію. Це можуть бути такі загрози, як: прослуховування розмов за допомогою спрямованих мікрофонів або інших пристроїв для акустичного знімання інформації, запис звуку, вібраційні загрози тощо.

Моделювання таких загроз включає визначення можливих шляхів витоку звуку, аналіз захищеності приміщень і систем від акустичних атак, а також розробку відповідних заходів захисту, таких як звукоізоляція або використання спеціальних шумопоглинальних матеріалів.

Рис. 3.6. Несанкціонований доступ до конфіденційної інформації з акустичного каналу витоку

Модель загроз для інформації через акустичний канал витоку фокусується на ризиках, пов'язаних із перехопленням звукових сигналів, що виникають під час розмов або переговорів. Основні загрози включають:

1. ***Акустичне підслуховування:*** використання мікрофонів або інших пристроїв для перехоплення звуків, що передаються в повітрі.
2. ***Віброакустичний витік:*** перехоплення звукових коливань через вібрації конструкцій, таких як стіни або вікна.
3. ***Електроакустичний перетворення:*** використання електронних пристроїв, які можуть перетворювати акустичні сигнали в електричні, дозволяючи передавати їх на відстань.

Мета моделі загроз полягає у виявленні та аналізі цих загроз для розробки ефективних заходів захисту, таких як звукоізоляція, антивібраційні матеріали та засоби глушіння сигналів.

Модель загроз для інформації через віброакустичний канал витоку

Модель загроз для інформації через віброакустичний канал витоку — це аналіз загроз, які виникають внаслідок перехоплення інформації через вібрації, що передаються через тверді поверхні (наприклад, стіни, підлогу, вікна) або конструкції, і можуть бути перетворені в аудіосигнали. Ці вібрації можуть виникати внаслідок звукових хвиль або діяльності обладнання та можуть бути використані для несанкціонованого отримання конфіденційної інформації.

Несанкціонований доступ до вмісту переговорів (розмов) зловмисниками може бути також здійснений (рис. 3.7) за допомогою стетоскопів і гідроакустичних датчиків.

Рис. 3.7. Несанкціонований доступ до вмісту переговорів

За допомогою стетоскопів можливе прослуховування переговорів через стіни товщиною до 1 м 20 см (залежно від матеріалу).

Залежно від виду каналу передачі інформації від самого вібродатчика стетоскопи підрозділяються на:

− провідні (провідний канал передачі);

− радіо - (передача по радіоканалу);

− інфрачервоні (інфрачервоний канал передачі).

Не виключена можливість використання і гідроакустичних датчиків, що дозволяють прослуховувати розмови в приміщеннях, використовуючи труби водопостачання і опалення. Правда, випадки застосування таких пристроїв на практиці дуже рідкі.

Модель загроз для інформації через віброакустичний канал витоку зосереджена на ризиках, пов'язаних із передаванням звукових коливань через вібрації конструкцій будівлі, таких як стіни, підлога, стеля та вікна. Основні загрози включають:

1. ***Перехоплення вібрацій:*** використання спеціальних пристроїв (наприклад, контактних мікрофонів), які виявляють і перетворюють вібрації конструкцій на звукові сигнали, що дозволяє підслуховувати розмови.
2. ***Передача вібрацій через будівельні матеріали:*** звукові коливання можуть поширюватися через тверді матеріали, створюючи ризик витоку інформації в суміжні приміщення.

Мета моделі загроз полягає в ідентифікації цих ризиків і розробці захисних заходів, таких як антивібраційна ізоляція, використання спеціальних матеріалів і структурні зміни, щоб зменшити можливість витоку інформації через вібрації.

Модель загроз для інформації за рахунок електроакустичного перетворення та обладнання в інформаційно-комунікаційній системі

В умовах сучасних інформаційно-комунікаційних систем, витік конфіденційної інформації під час переговорів може відбуватися через

електроакустичне перетворення в технічних засобах, які, хоча і не беруть безпосередньої участі в обробці інформації, можуть стати джерелом витоку. До таких "допоміжних засобів" належать телефонні апарати з дисковим номеронабирачем, телевізори, електронні годинники, підключені до системи синхронізації часу, та інші пристрої.

Основна загроза полягає в тому, що звукові коливання, які виникають під час розмови, можуть впливати на елементи електричних схем цих пристроїв, перетворюючи акустичні сигнали на електричні. Ці електричні сигнали потім передаються по провідних лініях (наприклад, телефонним або лініям синхронізації), що дозволяє зловмиснику отримати доступ до конфіденційної інформації на значній відстані від приміщення.

У випадку з телевізорами і приймачами, витік інформації відбувається через модуляцію частоти звуковими коливаннями, що випромінюються у вигляді електромагнітного поля. Це створює можливість перехоплення інформації через електромагнітне випромінювання пристроїв.

Для захисту від цих загроз в інформаційно-комунікаційній системі необхідно розробити і впровадити комплекс заходів, що включають фізичну ізоляцію приміщень, використання захисних екранів та спеціальних технічних засобів, що запобігають витоку інформації через електроакустичні канали. Це забезпечить надійний захист конфіденційної інформації під час проведення переговорів у таких приміщеннях.

Модель загроз для інформації з оптичного каналу та за рахунок високочастотного нав'язування в інформаційно-комунікаційній системі

В умовах інформаційно-комунікаційних систем, інформація, що обговорюється під час переговорів, може бути піддана загрозі витоку через оптичні канали та високочастотне нав'язування. Якщо приміщення для переговорів має вікна без захисних елементів (штор чи жалюзі), зловмисник може використовувати оптичні прилади з великим посиленням (наприклад, біноклі або підзорні труби) для перегляду приміщення і зчитування інформації.

Загроза через високочастотне нав'язування виникає, коли зловмисник підключає генератор частоти до телефонної лінії, що веде до приміщення. Генерований сигнал відбивається від телефонного апарата та модулюється розмовою, що ведеться в кімнаті. Отриманий сигнал може бути перехоплений і декодований на значній відстані.

Для захисту від цих загроз в інформаційно-комунікаційній системі необхідно реалізувати комплекс заходів, включаючи:

1. ***Фізичний захист:*** оснащення вікон приміщень захисними шторами або жалюзі, що запобігатиме перегляду приміщення ззовні.
2. ***Захист від високочастотного нав'язування:*** використання спеціальних захисних фільтрів та екранів для телефонних ліній, що запобігатимуть

підключенню сторонніх генераторів частоти.

3. ***Моніторинг і контроль:*** регулярні перевірки приміщення на наявність несанкціонованого обладнання та можливих каналів витоку.

Застосування цих заходів забезпечить надійний захист конфіденційної інформації під час переговорів і знизить ризик її витоку через оптичні та високочастотні канали.

Розробка заходів захисту

Передбачуваний зловмисник – це висококваліфікований фахівець, який має глибокі знання про різні канали витоку інформації в приміщеннях для ведення переговорів. Він володіє професійними навичками і засобами для здобування конфіденційної інформації. Враховуючи такі загрози, необхідно розробити і впровадити комплекс заходів, які забезпечать надійний захист під час проведення переговорів та розмов.

Основні заходи захисту включають:

1. ***Фізичний захист приміщень:***
   - ✓ Встановлення штор, жалюзі або іншого захисного обладнання на вікнах для запобігання перегляду ззовні.
   - ✓ Обладнання приміщень звукоізоляційними матеріалами для зниження можливості прослуховування через стіни або інші будівельні конструкції.
2. ***Захист від високочастотного нав'язування:***
   - ✓ Встановлення фільтрів на телефонні лінії для запобігання підключення генераторів частоти.
   - ✓ Використання екранів і захисних пристроїв, що знижують можливість модуляції сигналів під час переговорів.
3. ***Технічні засоби захисту:***
   - ✓ Регулярний моніторинг і сканування приміщень на наявність прихованих пристроїв прослуховування або зйомки.
   - ✓ Використання обладнання для виявлення несанкціонованих електромагнітних випромінювань і сигналів.
4. Організаційні заходи:
   - ✓ Обмеження доступу до приміщень для переговорів, включаючи встановлення системи контролю доступу.
   - ✓ Навчання персоналу з питань інформаційної безпеки, включаючи виявлення підозрілих дій і правильне поводження з конфіденційною інформацією.

Всі ці заходи в комплексі дозволять мінімізувати ризики витоку інформації під час проведення переговорів і забезпечити належний рівень захисту конфіденційних даних в інформаційно-комунікаційній системі.

3.4. Методи й засоби блокування каналів витоку інформації

Захист інформації від витоку технічними каналами включає проектно-архітектурні рішення, організаційні та технічні заходи, а також виявлення портативних закладних пристроїв.

1. **Організаційні заходи**:
   - ✓ Залучення ліцензованих організацій для захисту інформації.
   - ✓ Категорування та атестація об'єктів ТЗПІ.
   - ✓ Використання сертифікованих ТЗПІ та ДТЗС.
   - ✓ Встановлення контурів захисту (КЗ) навколо об'єкта.
   - ✓ Контроль доступу на об'єкти ТЗПІ та в виділені приміщення.
   - ✓ Введення обмежень у використанні технічних засобів.
   - ✓ Відключення технічних засобів з електроакустичними елементами під час секретних заходів.
2. **Технічні заходи**:
   - ❖ **Пасивні методи**:

1. Контроль доступу на об'єкти ТЗПІ.
2. Локалізація випромінювання (екранування, заземлення, звукоізоляція).
3. Розв'язування інформаційних сигналів (спеціальні захисні засоби, діелектричні вставки, автономні джерела живлення, фільтри).

   - ❖ **Активні методи**:

1. Просторове зашумлення (електромагнітне, акустичне, вібраційне).
2. Лінійне зашумлення (мережі електроживлення, сторонні дроти).
3. Знешкодження закладних пристроїв (генератори імпульсів).

3. **Виявлення закладних пристроїв**:
   - ✓ Пасивні методи: лазерні детектори, стаціонарні детектори диктофонів, індикатори поля.
   - ✓ Активні методи: нелінійні локатори, рентгенівські комплекси.

Комплексний підхід включає використання апаратних, програмних, криптографічних методів і організаційних заходів для забезпечення безпеки.

Методи виявлення закладних пристроїв:

❖ **Пасивні методи**:
- ✓ Лазерне підсвітлення скла на вікнах.
- ✓ Стаціонарні детектори диктофонів.
- ✓ Індикатори поля, інтерсептори, частотоміри, сканувальні приймачі та програмно-апаратні комплекси.
- ✓ Радіоконтроль побічних електромагнітних випромінювань ТЗПІ.

❖ **Активні методи**:
- ✓ Нелінійні локатори для перевірки приміщень.
- ✓ Рентгенівські комплекси для перевірки ТЗПІ та ДТЗІ.

3.5. Модель порушника безпеки інформації в ІКС

На підставі Акту обстеження та визначення загроз для інформаційно-комунікаційної системи (ІКС) СЗІ розробляє «Модель порушника безпеки інформації в ІКС», яка затверджується керівником організації-власника (розпорядника) ІКС та, за потреби, вноситься до відповідних розділів Плану захисту.

Модель порушника − це формалізований або неформалізований опис дій порушника, що відображає його можливості, знання, час та місце дії. Порушник − це особа, яка може отримати несанкціонований доступ до засобів ІКС.

Модель порушника визначає:

- цілі порушника та їх небезпечність для ІКС та інформації, що потребує захисту;
- категорії персоналу, користувачів ІКС та сторонніх осіб, які можуть бути порушниками;
- припущення щодо кваліфікації та характеру дій порушника.

Метою порушника можуть бути:

- отримання інформації;
- внесення змін до інформаційних потоків;
- знищення матеріальних та інформаційних цінностей.

Порушників поділяють на зовнішніх і внутрішніх. Зовнішніми порушниками можуть бути:

- добре оснащена група, що діє швидко;
- одиночні порушники, що діють обережно.

Сторонні особи, що можуть бути порушниками:

- клієнти;
- відвідувачі;
- представники взаємодіючих організацій;
- представники конкуруючих організацій або їх агенти;
- особи, які випадково або навмисно порушили пропускний режим.

Потенційні внутрішні порушники:

- допоміжний персонал;
- основний персонал;
- співробітники служби безпеки.

Мотиви порушень можуть бути:

- безвідповідальність;
- самоствердження;
- корисливий інтерес.

Порушників класифікують за:

- рівнем знань про ІКС;
- рівнем можливостей;
- часом дії;
- місцем дії.

Крім того, враховуються такі обмеження та припущення щодо дій можливих порушників:

- робота з підбору та розстановки кадрів ускладнює створення коаліцій порушників;
- порушник приховує свої несанкціоновані дії від інших співробітників;
- НСД може бути наслідком помилок користувачів, адміністраторів або хиб технології обробки інформації.

Припускається, що порушник – це фахівець вищої кваліфікації з повною інформацією про ІКС і засоби захисту.

Модель порушника визначає ймовірність реалізації загрози, своєчасність виявлення та відомості про порушення. Всі злочини, зокрема комп'ютерні, здійснюються людиною, тому безпека ІКС є питанням людських відносин та поведінки.

Модель порушника можна відобразити системою таблиць, використовуючи всі можливі категорії, ознаки та характеристики порушників для точного аналізу та оцінки загроз.

Таблиця 2. Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
	Внутрішні по відношенню до ІКС	
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІКС	1
ПВ2	Персонал, який обслуговує технічні засоби ІКС (інженери, техніки)	2
ПВ3	Користувачі (оператори) ІКС	2
ПВ4	Адміністратори ІКС, співробітники служби захисту інформації	3
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	4
	Зовнішні по відношенню до ІКС	
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів або закордонних спецслужб «під прикриттям»	4

Таблиця 3. Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов’язок (ПЗ4)	4

Таблиця 4. Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІКС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІКС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІКС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІКС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІКС, їх недоліки та можливості	4

Таблиця 5. Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІКС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІКС, дезорганізації систем обробки інформації	4

Таблиця 6. Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час повної бездіяльності ІКС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІКС з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІКС (або компонентів системи)	3
Ч4	Як у процесі функціонування ІКС, так і під час призупинки компонентів системи	4

Таблиця 7. Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до технічних засобів ІКС	1
Д2	З робочих місць користувачів (операторів) ІКС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІКС	4

Виведемо два варіанти сумарного рівня загроз для окремих категорій можливих порушників:

1) **Внутрішній порушник «ПВ»**

***Тип загрози*:** мінімальні загрози

Опис: внутрішній порушник — це співробітник або особа, яка має доступ до інформації в межах організації і порушує правила через безвідповідальне ставлення до своїх обов'язків. Це може проявлятися у вигляді недбалості, помилок при виконанні завдань або ігнорування процедур безпеки. Такі дії можуть випадково або ненавмисно призвести до витоку інформації або порушення її цілісності.;

2) **Зовнішній порушник «ПЗ4»**

Тип загрози: максимальні загрози

Опис: зовнішній порушник «ПЗ4» є агентом конкурентів або закордонних спецслужб, який діє під прикриттям. Цей тип порушника реалізує цілеспрямовані несанкціоновані дії з метою модифікації, крадіжки або іншого завдання шкоди важливій інформації. Такі дії часто мають серйозні наслідки для безпеки організації, оскільки вони включають складні методи атаки та ретельно сплановані операції для досягнення своїх цілей.

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
прибир	ПВ1	М1	К1	З1	Ч4	Д1	**9**
	1	1	1	1	4	1	
	ПЗ4	М4	К4	З4	Ч4	Д1	**21**
	4	4	4	4	4	1	
електр	ПВ1	М1	К1	З1	Ч1	Д1	**8**
	1	1	1	1	3	1	
	ПЗ4	М4	К4	З4	Ч1	Д1	**20**
	4	4	4	4	3	1	
технік	ПВ2	М1	К2	З1	Ч4	Д3	**12**
	2	1	2	1	4	2	
	ПЗ4	М4	К4	З4	Ч4	Д3	**22**
	4	4	4	4	4	2	
корист	ПВ3	М1	К2	З1	Ч3	Д2	**11**
	2	1	2	1	3	2	
	ПЗ4	М4	К4	З4	Ч3	Д2	**21**
	4	4	4	4	3	2	
адмініс	ПВ4	М1	К4	З1	Ч4	Д4	**17**
	3	1	4	1	4	4	
	ПЗ4	М4	К4	З4	Ч4	Д4	**24**
	4	4	4	4	4	4	
пе	ПВ5	М1	К1	З1	Ч4	Д3	**14**
	4	1	1	1	4	3	

	ПЗ4	М4	К4	З4	Ч4	Д3	**23**
	4	4	4	4	4	3	

Після зведення усіх даних 1-го варіанту в одну таблицю отримаємо таку табличну **«Модель внутрішнього порушника політики безпеки інформації»**:

Категорія порушника «ПВ»	Мотив порушень	Рівень обізнаності щодо ІКС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Служба безпеки	М1	К1	З1	Ч4	Д3	**14**
Адміністратор ІКС	М1	К4	З1	Ч4	Д4	**17**
Користувач	М1	К2	З1	Ч3	Д2	**11**
Технік ІКС	М1	К2	З1	Ч4	Д3	**12**
Електрик	М1	К1	З1	Ч1	Д1	**8**
Прибиральник	М1	К1	З1	Ч4	Д1	**9**

Висновок: з таблиці видно, що найбільшу загрозу для безпеки інформації в інформаційно-комунікаційній системі (ІКС) становить адміністратор. Саме його діяльність повинна бути під особливим контролем, оскільки він є основним потенційним порушником.

3.6. Модель загроз для інформації в ІКС

Після обстеження ІКС слід визначити потенційні загрози, які можуть мати випадкове або навмисне походження. Випадкові загрози виникають через непередбачені обставини, такі як стихійні лиха, відмови, збої, помилки або побічні впливи. Відмова призводить до несправності ІКС, збій — до тимчасового порушення її роботи, а помилка — до неправильного виконання функцій. Побічний вплив виникає через негативні фактори всередині або зовні системи.

Навмисні загрози з'являються через зловмисні дії, зокрема розвідку, шпигунство чи злочинні дії. Джерелами загроз можуть бути люди, технічні засоби, алгоритми, програми, зовнішнє середовище тощо.

Загрози класифікуються за доступом до ІКС та станом її функціонування. Враховуються як відомі загрози, так і потенційні нові загрози, які можуть виникнути внаслідок нових технологічних рішень. Модель загроз для ІКС визначає можливі типи загроз та способи їх реалізації, а також враховує фактори як об'єктивної, так і суб'єктивної природи. Випадкові загрози включають дії персоналу через необережність чи незнання, а навмисні − дії порушників, що спрямовані на доступ до ресурсів ІКС або дезорганізацію її роботи.

Зробимо розрахунок загроз з урахуванням 3-х рівнів ризиків і збитків:

- ✓ високий - якщо реалізація загрози надає великих збитків (3 бали);
- ✓ середній - якщо реалізація загрози надає помірних збитків (2 бали);
- ✓ низький - якщо реалізація загрози надає незначних збитків (1 бал).

Модель загроз з визначенням рівня ризиків та збитків

1. Загрози конфіденційності інформації

№	Механізм реалізації	Рівень		Сума загроз
		ризиків	збитків	
К.1	Ненавмисне ознайомлення з ІзОД під час співбесід персоналу ІКС зі сторонніми особами	середній 2	високий 3	5
К.2	Втрата носіїв ІзОД з причини безвідповідального ставлення до виконання обв'язків	низький 1	високий 3	4
К.3	Перегляд ІзОД на екранах моніторів або робочих місцях користувачів ІКС сторонніми особами	середній 2	високий 3	5
К.4	Копіювання ІзОД на зовнішні носії з метою несанкціонованого ознайомлення сторонніх осіб	високий 3	високий 3	6
К.5	Роздрукування ІзОД з метою несанкціонованого ознайомлення сторонніх осіб	середній 2	високий 3	5
К.6	Викрадення носіїв ІзОД з метою несанкціонованого ознайомлення сторонніх осіб	низький 1	високий 3	4
К.7	Безпосередній доступ до ІзОД будь-яким способом сторонніх осіб	низький 1	високий 3	4

2. Загрози цілісності інформації

№	Механізм реалізації	Рівень		Сума загроз
		ризиків	збитків	
Ц.1	Помилки (ненавмисні) користувачів ІКС, які призвели до модифікації або спотворення інформації на жорсткому диску або зовнішніх носіях	середній 2	середній 2	4
Ц.2	Несанкціонована (навмисне) модифікація або спотворення інформації персоналом ІКС на жорсткому диску або зовнішніх носіях	середній 2	середній 2	4

Ц.3	Ненавмисне пошкодження носіїв інформації користувачами АС, яке призвело до модифікації або спотворення інформації	середній 2	середній 2	4
Ц.4	Навмисне пошкодження носіїв інформації користувачами ІКС, яке призвело до модифікації або спотворення інформації	низький 1	середній 2	3
Ц.5	Помилки (ненавмисні) адміністраторів ІКС при налагодженні засобів захисту та системного ПЗ, в наслідок яких стала можливою модифікація ІзОД	середній 2	середній 2	4
Ц.6	Прояви помилок системного ПЗ, в наслідок яких стала можливою модифікація інформації або її спотворення користувачами	середній 2	середній 2	4
Ц.7	Безпосередній доступ до інформації будь-яким способом сторонніми особами	низький 1	середній 2	3

3. Загрози доступності інформації

№	Механізм реалізації	Рівень		Сума загроз
		ризиків	збитків	
Д.1	Помилки (ненавмисні) користувачів ІКС, які призвели до знищення інформації або втрати доступу до неї	середній 2	середній 2	4
Д.2	Помилки (ненавмисні) адміністраторів ІКС, які призвели до знищення інформації або втрати доступу	середній 2	середній 2	4
Д.3	Некоректне налагодження засобів захисту АБ, яке призвело до втрати доступу до інформації або ІКС	середній 2	середній 2	4
Д.4	Пошкодження парольних носіїв персоналом ІКС, що призвело до втрати доступу до інформації	середній 2	середній 2	4
Д.5	Навмисне пошкодження парольних носіїв персоналом ІКС, яке призвело до втрати доступу до інформації	середній 2	середній 2	4
Д.6	Прояви помилок системного ПЗ, яке призвело до втрати доступу до інформації або ІКС	середній 2	середній 2	4
Д.7	Безпосередній доступ до ІКС будь-яким способом сторонніх осіб	низький 1	середній 2	3

4. Загрози спостереженості ІКС

№	Механізм реалізації	Рівень		Сума загроз
		ризиків	збитків	
Н.1	Помилки (ненавмисні) персоналу ІКС, які призвели до втрати спостереженості	низький 1	середній 2	3
Н.2	Помилки (ненавмисні) адміністраторів ІКС, які призвели до втрати спостереженості	середній 2	високий 3	5
Н.3	Некоректне налагодження засобів захисту адміністраторами ІКС, яке призвело до втрати спостереженості	низький 1	високий 3	4
Н.4	Порушення спостережності користувачами ІКС внаслідок навмисного переповнення протоколів аудиту	середній 2	середній 2	4
Н.5	Порушення спостереженості внаслідок пошкодження, у тому числі навмисного, поточних протоколів аудиту, архівів та носіїв з архівами протоколів аудиту	низький 1	високий 3	4
Н.6	Прояви помилок системного ПЗ, яке призвело до втрати спостереженості	середній 2	високий 3	5
Н.7	Безпосередній доступ до ІКС будь-яким способом сторонніх осіб	низький 1	високий 3	4

Модель загроз з розрахунком сумарного рівня ризиків та збитків:

№	Види загроз	1	2	3	4	5	6	7	Сума загроз
1	конфіденційності	5	4	5	6	5	4	4	33
2	спостереженості	3	5	4	4	4	5	4	29
3	доступності	4	4	4	4	4	4	3	27
4	цілісності	4	4	4	3	4	4	3	25

Зробимо розрахунок загроз з урахуванням 3-х рівнів ризиків і збитків:
- високий - якщо реалізація загрози надає великих збитків (3 бали);
- середній - якщо реалізація загрози надає помірних збитків (2 бали);
- низький - якщо реалізація загрози надає незначних збитків (1 бал).

3.7. Зміст завдань системи захисту інформації в інформаційно-комунікаційних системах (ІКС)

Зміст завдань системи захисту інформації в інформаційно-комунікаційних системах (ІКС) полягає в конкретному визначенні об'єктів захисту, які включають матеріальні носії інформації, що надають підприємству конкурентні переваги. Ці об'єкти можуть включати документи,

матеріали, засоби обробки та передачі інформації, мережі зв'язку, а також працівників. Захист забезпечується шляхом регулювання доступу, порядку використання та зберігання цих об'єктів.

Захисні заходи здійснюються за допомогою технічних, програмних та організаційно-правових засобів. Технічні засоби включають кодовані замки, системи пропуску та пристрої контролю доступу. Програмні засоби регулюють доступ до інформації в комп'ютерних системах і мережах. Правові засоби встановлюють порядок роботи з інформаційними ресурсами та правила використання технічних і програмних засобів захисту. Система захисту орієнтована на використання всіх доступних засобів для ефективного протистояння загрозам.

Таблиця 7. Зміст завдань системи захисту інформації

ЗАВДАННЯ	
Правового характеру	• регулювання доступу до інформаційних ресурсів суб'єкта підприємництва представників державних органів і установ; • регулювання доступу персоналу до інформаційних ресурсів суб'єкта підприємництва; • встановлення відповідальності за посягання на інформаційні ресурси суб'єкта підприємництва
Криптографічного характеру	• шифрування інформації при передачі її через незахищені засоби зв'язку; • регламентація доступу до баз даних та електронних документів
Організаційного характеру	• категоріювання інформації суб'єкта підприємництва • встановлення відповідного режиму роботи суб'єкта підприємництва; • організація спеціального діловодства в діяльності суб'єкта підприємництва; • підбір персоналу для роботи з інформацією, що має обмежений доступ; • профілактична та виховна робота з персоналом; • здійснення заходів захисту інформації у ході зустрічей, ділових переговорів, конференцій і т. і.; • планування дій щодо захисту інформації при стихійних лихах, пожежах, терористичних актах, інших негараздах
Інженернотехнічного характеру	• спеціальне інженерно-технічне обладнання місць зберігання інформації; • застосування спеціальних технічних засобів для перекриття різних видів каналів витоку інформації; • застосування технічних засобів охорони та технічна укріпленість об'єктів
Програмно-апаратного характеру	• застосування спеціальних програмних засобів захисту комп'ютерної інформації; • застосування антивірусних програм; • забезпечення безперебійної роботи комп'ютерних систем при аварійних ситуаціях; • виключення можливості перехоплення електромагнітних випромінювань і наводок;

	• створення системи страхового копіювання комп’ютерної інформації

4. ЗАВДАННЯ НА КУРСОВУ РОБОТУ

Необхідно провести дослідження об’єкта, його приміщень, роботу з документами в твердому і електронному вигляді, дати оцінку захищеності об’єкта від витоку інформації по технічним каналам і сформувати рекомендації по захисту інформації на об’єкті. Приміщення студент обирає самостійно, моделюючи потрібну ситуацію. Описати та представити склад та опис виявленних функціональних каналів витоку інформації. Визначити загрози і можливості порушника по перехопленню іформації (мовної, електронної, паперової тощо). На підставі проведеного аналізу представити вимоги до системи захисту інформації та розробити комплекс заходів, що забезпечують надійний захист.

Завдання:

Розділ 1. Структуризація інформації, що захищається

1. Розробити детальну структуру інформації, що потребує захисту, включаючи класифікацію за рівнем конфіденційності та критичності.
2. Визначити основні категорії та види даних, що підлягають захисту.

Розділ 2. Аналіз та моделювання можливих каналів витоку інформації на обраному об'єкті захисту

1. Проаналізувати потенційні канали витоку інформації на об'єкті захисту.
2. Моделювати параметри цих каналів для визначення можливих загроз та вразливостей.

Розділ 3. Оцінка ступеня загрози інформації, що захищається

1. Розробити модель потенційного порушника безпеки інформації, враховуючи його можливості та методи атаки.
2. Оцінити можливі сценарії атаки і їх вплив на систему захисту.
3. Провести моделювання загроз і ризиків для системи захисту інформації, враховуючи різні сценарії атак.
4. Оцінити ймовірність та наслідки можливих загроз для інформаційних систем.

Розділ 4. Розробка заходів щодо захисту інформації на об'єкті захисту

1. Розробити і описати заходи захисту для виявлених загроз, включаючи технічні і організаційні рішення.
2. Вибрати програмні рішення для захисту інформації, такі як системи моніторингу, антивірусні програми, і засоби шифрування.
3. Визначити апаратні рішення для забезпечення фізичного захисту, включаючи системи контролю доступу і моніторингу.
4. Впровадити системи шифрування для захисту даних при їх зберіганні і передачі. Вибрати алгоритми шифрування, такі як AES або RSA, відповідно до рівня безпеки.

5. Вибрати і впровадити програмне забезпечення для захисту від вірусів та шкідливого ПЗ. Налаштувати регулярні оновлення баз даних вірусів і здійснювати сканування системи.
6. Налаштувати фаєрволи для контролю і фільтрації вхідного та вихідного трафіку. Впровадити правила доступу і блокування небезпечних портів.
7. Встановити і налаштувати IDS/IPS системи для моніторингу і реагування на підозрілу активність в мережі. Забезпечити регулярний моніторинг і аналіз записів.
8. Створити політики інформаційної безпеки, що охоплюють всі аспекти захисту інформації, включаючи обробку даних і доступ до них.
9. Організувати навчання для персоналу з питань інформаційної безпеки, включаючи розпізнавання фішинг-атак і дотримання політик безпеки.
10. Розробити і документувати процедури реагування на інциденти безпеки, включаючи виявлення, аналіз і усунення інцидентів.
11. Визначити технічні засоби для захисту критичних систем і даних від фізичного доступу. Це можуть бути системи контролю доступу, відеоспостереження, замки та інші засоби фізичної безпеки.
12. Розробити комплексні заходи захисту інформації на об'єкті, включаючи організаційні та технічні рішення.
13. Оцінити ступінь захищеності інформації та ефективність запропонованих заходів.

Розділ 5. Схема та вибір розміщення технічних засобів захисту інформації на об'єкті

1. Розробити просторову та структурну модель приміщення для забезпечення фізичного захисту інформації (наприклад, для переговорів).
2. Визначити оптимальне розміщення технічних засобів захисту інформації в приміщенні.
3. Розробити схему розміщення технічних засобів захисту, таких як датчики, системи контролю доступу, обладнання для моніторингу та фільтрації трафіку.
4. Провести розрахунки для визначення оптимального розміщення засобів захисту для максимізації ефективності при мінімальних витратах.
5. Розробити план інтеграції нових технічних засобів з існуючими інформаційними системами. Забезпечити сумісність і ефективність роботи нових і існуючих систем.
6. Забезпечити можливість масштабування технічних засобів у разі необхідності. Врахувати можливості для розширення системи захисту в майбутньому.
7. Вибрати і розмістити обладнання для моніторингу трафіку, таке як мережеві монітори та аналітики.
8. Розмістити датчики для виявлення несанкціонованого доступу і системи контролю доступу у критичних точках.

9. Провести оцінку ефективності розміщення технічних засобів захисту, перевірити їх роботу в реальних умовах.
10. Внести корективи у схему розміщення на основі отриманих результатів, забезпечити максимальну ефективність захисту.

Курсова робота повинна містити:

- Огляд і аналіз систем обробки інформації на об'єкті.
- Структуризацію та класифікацію інформації, що потребує захисту.
- Моделі загроз і канали витоку інформації.
- Методи і засоби блокування витоків інформації.
- Модель порушника безпеки і сценарії атаки.
- Просторову і структурну модель приміщення для фізичного захисту.
- Програмні і апаратні рішення для захисту інформації.
- Результати моделювання загроз і ризиків.
- Розроблені заходи захисту та оцінка їх ефективності.

5. ВИМОГИ ДО ОФОРМЛЕННЯ ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

5.1. Загальні вимоги

Курсова робота повинна містити графічну частину і записку пояснення.

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.

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

5.2. 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.

5.3. 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)_____

5.4. 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). Кожна схема виконується на окремому листі формату А4.

5.5. 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.

5.6. 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 І та О.

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.

5.7. 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 рис. 4.1». За необхідності під ілюстрацією розміщують пояснювальні дані. Ілюстрація позначається словом «Рисунок», яке разом з назвою ілюстрації розміщують після пояснювальних даних, наприклад, «Рис. 2.16. Схема криптографічного захисту інформації». 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 (приклад наведено).

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

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.

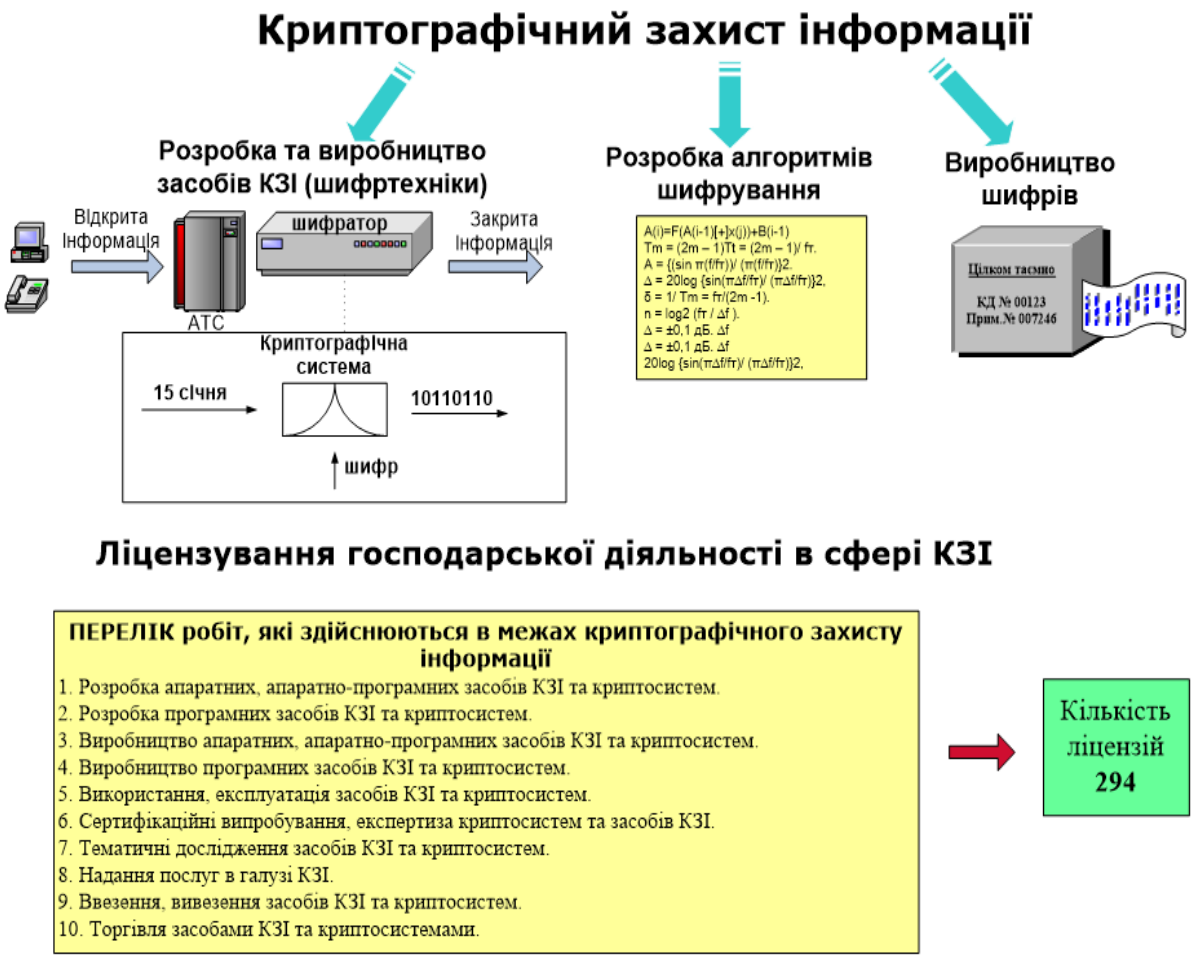


Рис. 2.16. Схема криптографічного захисту інформації

5.8. 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, наприклад, таблиця 3.1 − перша таблиця третього розділу. Номер таблиці від назви виділяють тире. Приклад оформлення таблиці наведено нижче на рисунку.

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. 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. 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.

Таблиця 2.4. Загасання від середовища поширення сигналу

Найменування	**Од. вим.**	**Значення**
1	**2**	**3**
Вікно в цегляній стіні	дБ	2
Стекло в металевій рамі	дБ	6
Офісна стіна	дБ	6
Залізні двері в офісній стіні	дБ	7
Залізні двері в цегляній стіні	дБ	12,4
Скловолокно	дБ	0,5-1
Стекло	дБ	3-20
Дощ і туман	дБ/км	0,02-0,05
Дерева	дБ/м	0,35
Кабельна зборка pigtale	дБ	0,5
Смуговий фільтр NCS F24XXX	дБ	1,5
Коаксіальний кабель	дБ/м	0,3
Роз'їм N - type	дБ	0,75
Інжектор живлення	дБ	0,5

6. 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 проєктуванні КР, встановлюється за 100-бальною шкалою із подальшим

переведенням її у наступну шкалу оцінок:

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

7. 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).

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. Процедура захисту передбачає стислий виклад студентом головних проблем дослідження роботи та їх рішення упродовж 10-15 хвилин та відповідей на запитання.

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.

8. ДОТРИМАННЯ ПРИНЦИПІВ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

При виконанні курсової роботи студенти повинні дотримуватись принципів академічної доброчесності. Курсову роботу студент має виконувати самостійно. Необхідно дотримуватись етики цитування, давати посилання на використані джерела, подавати достовірну інформацію про виконану роботу та її результати. У разі виявлення порушення студентом академічної доброчесності, зокрема академічного плагіату, фабрикації, фальсифікації, кваліфікаційна робота не допускається до захисту, а якщо такі факти були виявлені під час захисту, робота оцінюється на «незадовільно».

Студент зобов’язаний у терміни, визначені графіком освітнього процесу та розкладом екзаменів, допрацювати роботу та ліквідувати академічну заборгованість у визначеному порядку.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Жилін А. В. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

2. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

3. Г.М. Гулак, О.Б. Жильцов, П.М. Складанний, Р.В. Киричок, Н.В. Коршун. Інформаційна та кібернетична безпека підприємства / Навчальний підручник. КУБГ. – К. 2022. 451с.

4. Безпека інформації: конспект лекцій / укладач О. С. Кушнерьов. – Суми: Сумський державний університет, 2021. – 99 с.

5. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.

Додатковий

5. Комплексні системи захисту інформації: навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця: ВНТУ, 2018. – 118 с.

6. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах: навч. посіб. — Кропивницький: Видавець Лисенко В. Ф., 2020. — 295 с.

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

8. Технології захисту інформації / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці: Чернівецький національний університет, 2013. – 471 с.

9. Основи інформаційної безпеки [Текст]: навч. пос. / Дудикевич В. Б., Хорошко В.О., Яремчук Ю.Є. – Вінниця: ВНТУ, 2018. – 316 с.

10. Основи кібербезпеки та кібероборони: підручник / Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.

Інтернет-ресурси

11. Курси Cisco Packet Tracer.
https://www.netacad.com/ua/courses/packet-tracer

ДОДАТКИ

ДОДАТОК А

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

КУРСОВА РОБОТА
З ДИСЦИПЛІНИ
«ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»
НА ТЕМУ:

Студента (ки) _____ курсу ___ _____ ___ групи
освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем
спеціальності 125 Кібербезпека та захист інформації
_____
(ПІБ)
Науковий керівник: _____
_____
(посада, вчене звання, науковий ступінь, ПІБ)

Національна шкала _____

Кількість балів: _____ Оцінка: ECTS_____

_____ _____
(підпис) (ім'я, прізвище)

Київ 20___

ДОДАТОК Б

Київський столичний університет імені Бориса Грінченка

Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Дисципліна Захист інформації в інформаційно-комунікаційних системах

Курс _____ Група _____Семестр____

Затверджую
Зав. кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
к.т.н., доц. Складанний П.М.
«___ » _____

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 на кафедру _____
5. Термін захисту курсової роботи _____
6. Дата видачі завдання _____

Студент_____
(підпис) (ім'я, прізвище)
Науковий керівник _____ _____
(підпис) (ім'я, прізвище)

Завідувач кафедри _____ _____
(підпис) (ім'я, прізвище)

ДОДАТОК В

Київський столичний університет імені Бориса Грінченка

Рецензія на курсову роботу і результат захисту

Студента _____
(прізвище, ім'я та по батькові)

_III_курсу _____ групи факультету інформаційних технологій та математики

Курсова робота з з дисципліни «Захист інформації в інформаційно-комунікаційних системах»

Тема _____

Реєстраційний № _____, дата одержання «____» _____ 20___ р.

Науковий керівник _____
(вчене звання, прізвище, ініціали)

Зміст рецензії

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
_____
_____
_____
_____

Допущено до захисту «___»_____ 20____ р.

Захист планується «_____»_____20____ р.

_____
(підпис наукового керівника)

Курсова робота захищена «_____» _____20____р.

з оцінкою _____
(за національною шкалою та шкалою ЄКТС)

_____ PhD, Юлія КОСТЮК
(підпис) (ім'я, прізвище)

Приклад анотації

АНОТАЦІЯ

Курсова робота виконана студентом Івановим Іваном Івановичем на тему «Організація захисту персональних даних в інформаційно-комунікаційній системі туристичного підприємства». Дослідження присвячене розробці та впровадженню комплексної системи захисту персональних даних у туристичній сфері, з особливим акцентом на забезпеченні конфіденційності, цілісності та доступності інформації клієнтів і співробітників.

У роботі детально розглядаються сучасні методи захисту інформаційно-комунікаційних систем, зокрема використання шифрування даних, управління доступом, автентифікації користувачів, а також впровадження систем виявлення і запобігання вторгненням. Особливу увагу приділено специфіці захисту інформації у сфері туризму, де обробка та зберігання великого обсягу персональних даних клієнтів вимагає особливо високого рівня безпеки.

З огляду на постійне зростання кількості кіберзагроз та випадків витоку даних, у роботі акцентується на необхідності впровадження надійних заходів захисту, що дозволять забезпечити стійкість інформаційно-комунікаційних систем туристичного підприємства до сучасних загроз. Забезпечення конфіденційності, цілісності та доступності персональних даних є пріоритетним завданням для туристичних компаній, які прагнуть зберегти свою репутацію та уникнути можливих фінансових і юридичних наслідків витоку інформації. Окрема увага приділяється розробці політик і процедур безпеки, спрямованих на мінімізацію ризиків

Робота складається зі вступу, чотирьох розділів, висновків та пропозицій, списку використаних джерел, який складається з 17 найменувань, 8 додатків. Робота містить 5 рисунків і 8 таблиць. Загальний обсяг роботи становить 39 сторінок

Метою курсової роботи є розробка комплексної системи захисту персональних даних в інформаційно-комунікаційній системі туристичного підприємства, яка забезпечить надійний захист інформації від несанкціонованого доступу, кібератак та інших загроз, а також гарантуватиме безпечну роботу та захист конфіденційної інформації.

Об'єктом дослідження є інформаційно-комунікаційна система туристичного підприємства, її структура, технологічні рішення та засоби забезпечення інформаційної безпеки.

Ключові слова: захист персональних даних, інформаційно-комунікаційні системи, туристичне підприємство, інформаційна безпека, кіберзагрози, шифрування даних, управління доступом, автентифікація.

ДОДАТОК Г

Приклад оформлення

Перелік умовних позначень, символів, одиниць, скорочень і термінів

ОІД – об'єкт інформаційної діяльності
ЗЗІ – засоби захисту інформації
ТЗІ – технічний захист інформації
АС – автоматизована система
ІзОД – інформація з обмеженим доступом
НСД – несанкціонований доступ
ПЕМВН – побічні електромагнітні випромінювання і наводки
ОІД – об’єкт інформаційної діяльності
ОТЗ – основні технічні засоби
ДТЗ – допоміжні технічні засоби
ПМА – програма і методика випробувань
НД ТЗІ – нормативний документ системи технічного захисту інформації
КЗЗ – комплекс засобів захисту
АЗ – апаратне забезпечення
ПБ – політика безпеки
ТЗ – технічне завдання
DLP – Data Leak Prevention
IPS – Intrusion prevention system
IDS – Intrusion detection system
SIEM – security information & event management
ADM – architecture develop method
КПЕ – ключові показники ефективності

ДОДАТОК Д

Шаблон для формування змісту

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

4. **Завдання дослідження** – вони пишуться для того, щоб за допомогою їх вирішення можна було досягти мети, яку ми ставимо в роботі. Тобто для досягнення мети роботи слід вивчити, описати, показати, визначити, встановити, досліджувати, розглянути, розробити, розкрити, висвітлити, виявити, проаналізувати, довести, узагальнити що-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. **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.

7. **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

Електронна пошта, в даний час, є одним з найважливіших інформаційних ресурсів мережі Internet – засобом електронних комунікацій, основним призначенням якої є можливість спілкуватися користувачам один з одним.

Фактично появу електронної пошти можна віднести до 1965 року, коли співробітники Массачусетського технологічного інституту (MIT) Ноель Морріс і Том Ван Вабив написали програму MAIL для операційної системи CTSS (Compatible Time-Sharing System), яка була встановлена на комп'ютері IBM 7090/7094.

Потім, протягом багатьох років створювалися нові поштові програми, які постійно вдосконалювалися.

Наприклад, в 1971 році Рей Томлінсон, співробітник компанії “Bolt Beranek and Newman, Inc.” (BBN), розробив поштову програму для пересилки повідомлень по розподіленої мережі. А в 1972 році, він же модернізував її, адаптувавши для використання в мережі ARPANET, яка була попередницею нинішньої мережі Інтернет. Саме в цей час в адресах електронної пошти став використовуватися символ «@».

Перша ж програма, яка дозволяла створювати і сортувати списки листів, зберігати повідомлення в файлі, а також пересилати електронні листи на іншу адресу або автоматично відповідати на отримане послання, була розроблена вже Ларрі Робертсом.

Поступово налаштовувалася електронний поштовий зв’язок між різними країнами і континентами, дозволяючи людям обмінюватися електронними листами на величезних відстанях.

У міру зростання популярності електронної пошти стали з’являтися також різні шкідливі об’єкти, які роблять пошту вразливою, такі як віруси і спам, поширювані через мережу.

Перший спам був розісланий в 1994 році, будучи тоді першої розсилкою рекламних оголошень, які мають зараз своє поширена назва і статус – розсилки “засмічують” поштові скриньки користувачів непотрібною інформацією.

Таким чином, електронний спосіб відправлення та отримання листів не здає своїх позицій і, на сьогоднішній день, мільйони людей використовують електронну пошту як спосіб зв’язку.

Актуальність. У сучасних умовах життя, коли необхідно швидко реагувати на події, що відбуваються в світі, використання електронної пошти незамінне. Особливо це стосується ділової сфери. Електронна пошта може застосовуватися в різних цілях. Наприклад, для інформаційної підтримки споживачів або рекламування товарів і послуг.

У зв’язку з цим використання електронної пошти є актуальним. Вона повинна забезпечувати користувачеві виконання всіх основних функцій:

– Доставку листів;

– Відправлення повідомлень.

З використанням електронної пошти, з’явилася необхідність вивчення основних її характеристик і принципів роботи, а також способів захисту від шкідливих об’єктів.

Мета курсової роботи – охарактеризувати поняття «електронна пошта» і вивчити принципи її роботи.

Завдання курсової роботи:

– Розкрити поняття «електронна пошта»

– Показати основні переваги використання електронної пошти;

– Виявити недоліки електронної пошти;

– Виявити необхідність в захисті електронної пошти від вірусів і спаму;

– Визначити основні шляхи вирішення проблеми захисту поштової скриньки.

– Вивчити, на підставі, яких протоколів функціонує сервіс електронної пошти.

Об’єктом дослідження процес забезпечення безпеки електронної поштаи в цілому.

Предмет дослідження – підходи, методи та інструменти забезпечення безпеки роботи електронної пошти, її програмних і апаратних компонентів.

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

ДОДАТОК К

ЗРАЗКИ ОФОРМЛЕННЯ БІБЛІОГРАФІЧНИХ ОПИСІВ У СПИСКУ ВИКОРИСТАНИХ ДЖЕРЕЛ

1.Захист інформації в автоматизованих системах управління: навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2017. – 226 с.

2.Управління інформаційною безпекою: конспект лекцій [Електронний ресурс]: навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021. – 258 с.

3.Жилін А.В., Шаповал О.М., Успенський О.А. Технології захисту інформації в інформаційно-телекомунікаційних системах. Київ: КПІ ім. Ігоря Сікорського, 2020. С. 39 – 154.

4.Stallings W. “Cryptography and Network Security: Principles and Practice”. Pearson. 2017. pp. 85 – 517.

5.Азарова А. О, Дьогтєва І. О, Шиян А. А Система підтримки прийняття рішень щодо підвищення рівня інформаційної безпеки підприємства. Інформаційні технології та комп'ютерна інженерія. 2022. № 1. С. 12–18.

6.Інформаційна безпека now: яких елементів не вистачає? URL: https://ecpl.com.ua/news/informatsiyna-bezpeka-now-iakykh-elementiv-ne-vystachaie/.

7.Кухарська Н. П., Полотай О. І. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. Збірник "Information Technology and Security". 2019. Вип. 7. № 2 (13). С. 126–136. URL: https://sci.ldubgd.edu.ua/jspui/handle/123456789/7172.

8.Кунєв Ю. Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. Юридичний вісник "Повітряне і космічне право". 2021. № 1 (58). С. 95–102.
URL: https://dspace.nau.edu.ua/bitstream /NAU/53719/1/%d0%ae.%20%d0%94.%20%d0%9a%d1%83%d0%bd%d1%94%d0%b2.pdf.

9.Панченко О. А. Інформаційна безпека в контексті викликів і загроз національній безпеці. Публічне управління та місцеве самоврядування. 2020. № 2. С. 57–63.

10. Захарченко М.В. Інформаційна безпека інформаційно-комунікаційних систем. Захист інформації від НСД у каналах зв’язку: навч. посіб. / М.В. Захарченко, В.В. Топалов, М.С. Русляченко // За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2014. – 228 с.

11. Міночкін А.І., Романюк О.Н. Методи та моделі розпізнавання кібератак. Кібербезпека: освіта, наука, техніка. 2021. No 1. С. 36-45.

ДОДАТОК Л

ПРИКЛАД ЗАЯВИ НА ЗАТВЕРДЖЕННЯ ТЕМИ КУРСОВОЇ РОБОТИ

Завідувачу кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
к.т.н., доц. Складанному П.М.
студента групи_______
спеціальності 125 «Кібербезпека та захист інформації»
Іванова Івана Івановича

ЗАЯВА

Прошу затвердити тему курсової роботи «Організація захисту персональних даних в інформаційно-комунікаційній системі туристичного підприємства» з дисципліни «Захист інформації в інформаційно-комунікаційних системах» та призначити керівником курсової роботи Костюк Ю.В.

«_____»_____ _____