Теми кваліфікаційних робіт другого(магістерського) рівня вищої освіти освітньо-професійної програми

«Управління інформаційною та кібернетичною безпекою»

1. Методи та засоби проведення аудиту системи управління пристроїв та баз даних організації.
2. Методи та засоби забезпечення безпеки IT ресурсів в системах електронних платежів банків.
3. Технологія створення системи управління інформаційною безпекою в організації.
4. Методи забезпечення захисту мовної інформації в каналах зв'язку та передачі даних.
5. Технологія захисту компонентів IoT системи у критичній інфраструктурі.
6. Розробка і методики використання метрик в оцінці інформаційної безпеки на підприємстві.
7. Технології і продукти в архітектурі систем забезпечення інформаційної безпеки на підприємстві та оцінка їх можливостей у використанні.
8. Розробка документів політики інформаційної безпеки на підприємстві.
9. Організація процесів управління ризиками інформаційної безпеки та методики вимірювання їх показників ефективності.
10. Системи управління інформацією та подіями (SIEM) у забезпеченні інформаційної безпеки підприємства та методики оцінки її ефективності.
11. Організація перевірки СУІБ підприємства на відповідність вимогам міжнародних стандартів та методика її оцінки.
12. Організація заходів по виявленню загроз і інцидентів інформаційної безпеки на підприємстві та їх оцінка.

13. Організація впровадження системи управління безперервністю бізнесом і інцидентами інформаційної безпеки на підприємстві та їх оцінка.
14. Розробка системи управління інформаційною безпекою підприємства з використанням методів штучного інтелекту.
15. Оцінка ефективності програм захисту інформації в організації.
16. Методика розробки та впровадження системи управління інформаційною безпекою в організації на основі міжнародних стандартів та нормативних вимог.
17. Дослідження можливостей використання алгоритмів машинного навчання для автоматизації управління кібербезпекою в організаціях.
18. Аналіз впливу людського фактору на ефективність захисту інформації в організаціях.
19. Аналіз впливу штучного інтелекту на кібербезпеку та захист інформації.
20. Створення моделі культури кібербезпеки в організації.
21. Розробка системи виявлення загроз з використанням машинного навчання.
22. Розробка моделі машинного навчання для виявлення аномальних дій та потенційних кіберзагроз у комп'ютерних системах.
23. Застосування штучного інтелекту в системах ідентифікації та автентифікації.
24. Розробка системи прогнозування кібератак з використанням аналізу даних та штучного інтелекту.
25. Оцінка ефективності інструментів штучного інтелекту для виявлення, аналізу та розслідування кіберінцидентів.
26. Застосування нейронних мереж для захисту інформації в хмарних сервісах.
27. Розробка алгоритмів для автоматизованої аналітики кіберзагроз з використанням штучного інтелекту.

28. Розробка методів та алгоритмів штучного інтелекту для прогнозування та оцінки ризиків в галузі інформаційної безпеки.
29. Застосування блокчейн технологій для забезпечення кібербезпеки.
30. Використання штучного інтелекту для підвищення ефективності управління кібербезпекою в організації.
31. Створення СКУД малого підприємства з використанням технологій біометричної ідентифікації.
32. Технології виявлення та запобігання загрозам соціальної інженерії для підприємства: порівняльний аналіз.
33. Технології введення в оману (Deception Technology) у забезпеченні кібербезпеки підприємства.
34. Технології симуляційного навчання у запобіганні загрозам соціальної інженерії підприємства: порівняльний аналіз рішень від провідних виробників.
35. Організація роботи червоної та синьої команд забезпечення кібербезпеки підприємства.
36. Розробка і впровадження стратегії кіберстійкості сучасного підприємства.
37. Напрями забезпечення кіберстійкості держави відповідно до законодавства провідних держав світу та ЄС.
38. Забезпечення конфіденційності в мережі Інтернет: проблеми та шляхи їх вирішення.
39. Управління безпекою даних підприємства за використання мультихмарного середовища.
40. Управління доступом до інформаційних ресурсів на підприємстві.
41. Захист мережевого доступу до ресурсів підприємства.
42. Стратегічні орієнтири управління інформаційною безпекою організацій на шляху до євроінтеграції.
43. Управління інформаційною безпекою банків: політика та моніторинг її дотримання.

44. Управління безпекою інформації в хмарних сервісах.
45. Забезпечення безпеки інформаційного середовища підприємства.
46. Розробка та впровадження методики тестування захищеності критичної інфраструктури.
47. Аналіз ефективності стратегій Red Teaming у фінансових установах: виклики та можливості.
48. Створення моделі Security Operation Center для забезпечення кібербезпеки в банківській сфері.
49. Порівняльний аналіз підходів до тестування безпеки хмарних інфраструктур у підприємств та організацій.
50. Організація процесу впровадження Red Team на підприємстві: стратегічні підходи та практичні виклики.
51. Розробка імітаційної моделі для навчання персоналу Security Operation Center на прикладі банківських установ.
52. Аналіз та оцінка методів тестування безпеки SCADA у критичній інфраструктурі.
53. Впровадження системи моніторингу та аналізу кіберзагроз для підвищення ефективності реагування Security Operation Center у банківському секторі.
54. Дослідження методів оцінки ризиків та управління кібербезпекою в енергетичному секторі.