



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

Кафедра «Кібербезпека та захист інформації»

МЕТОДИЧНІ ВКАЗІВКИ
до курсового проекту
освітнього компонента (навчальної дисципліни)
СУЧАСНІ КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ
ІНФОРМАЦІЇ ТА ЇХ ОСОБЛИВОСТІ

назва освітнього компонента (навчальної дисципліни)

обов'язковий компонент циклу професійної підготовки

Рівень вищої освіти	<u>другий (магістерський)</u> перший (бакалаврський), другий (магістерський), третій (освітньо-науковий)
Форма здобуття освіти	<u>очна (денна)</u> очна (денна), заочна, дистанційна
Мова викладання	<u>Українська</u>

2025/2026 навчальний рік

Методичні вказівки до курсового проекту освітнього компонента (навчальної дисципліни) **«Сучасні КСЗІ та їх особливості»** для здобувачів очної (денної) форми здобуття освіти другого (магістерського) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації галузі знань F Інформаційні технології / Укл.: Зоріло В.В. – Одеса, 2025. – 29 с.

Розробник: Зоріло Вікторія Вікторівна, доцент кафедри «Кібербезпека та захист інформації»

Схвалено на засіданні кафедри «Кібербезпека та захист інформації»
Протокол від №2 від 06.10.2025.

Схвалено на засіданні НМК ННІ ІТІП
Протокол від №2 від 14.10.2025

ЗМІСТ

МЕТА ЗАВДАННЯ КУРСОВОЇ РОБОТИ.....	4
ПРИКЛАДИ ТЕМ КУРСОВОЇ РОБОТИ ТЕХНІЧНОЇ СПРЯМОВАНOSTІ...	4
РОЗДІЛИ КУРСОВОГО ПРОЕКТУ	6
СТРУКТУРА ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ.....	7
КРИТЕРІЇ ОЦІНЮВАННЯ КУРСОВОЇ РОБОТИ	8
ОФОРМЛЕННЯ ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ.....	13
ВИКОРИСТАНІ ДЖЕРЕЛА	24
ДОДАТОК 1.....	27
ДОДАТОК 2.....	28
ДОДАТОК 3.....	29

Мета завдання курсової роботи

Метою курсової роботи є набуття загальних та спеціальних компетентностей майбутніх магістрів, поглиблення теоретичних і практичних знань з використання сучасних підходів до оцінки захищеності інформаційної системи задля побудови КСЗІ.

При виконанні курсової роботи обрано наступний підхід: протягом 1-3 тижнів здобувач збирає інформацію про підприємство, де проходив переддипломну практику, або пропонує та узгоджує з викладачем інше підприємство, яке має бути доступним для здобувача та надавати йому усю необхідну інформацію. Опісля цього здобувач вищої освіти отримує від викладача деталізоване завдання на курсову роботу.

Приклади тем курсової роботи технічної спрямованості

1. Проектування комплексної системи захисту інформації для науково-дослідницької лабораторії кафедри кібербезпеки та програмного забезпечення Державного університету «Одеська політехніка».
2. Проектування комплексної системи захисту інформації для агентства туристичних послуг «TripMyDreem».
3. Проектування комплексної системи захисту інформації для фармацевтичної компанії «Анкор».

Загальний вигляд теми: «Проектування комплексної системи захисту інформації для [«Ваше підприємство»]».

Можливі підприємства:

1. Агентство нерухомості
2. Банківське відділення

3. Конструкторське бюро
4. Підприємство з виробництва зброї
5. Букмекерська контора
6. Провайдер Інтернет-послуг
7. Секретне підприємство
8. Науково-дослідний інститут
9. Підприємство з виготовлення програмного забезпечення
10. Підприємство з обробки алмазів.
11. Підприємство з виробництва коштовностей.
12. Статистичне управління.
13. Медичний заклад.
14. Фармацевтичний завод.
15. Аптека.
16. Рекламна агенція.
17. Компанія з виробництва цукерок.
18. Туристичне агентство.
19. Готельний бізнес.
20. Підприємство з розробки ландшафтного дизайну.
21. Обслуговування фермерських господарств насінням.
22. Офіційне представництво з продажу та обслуговуванню автомобілів.
23. Підприємство тюнінгу автомобілів.
24. Архітектурний інститут.
25. Надання послуг пов'язаних з ІТ.
26. Книжний магазин.
27. Юридична консультація.
28. Обслуговування касових апаратів.
29. Супермаркет.
30. Фабрика з пошиття одягу на експорт.

Розділи курсового проекту

1. При виконанні курсового проекту обов'язково повинні бути використані такі елементи:

- аналіз об'єкта захисту відповідно до НД ТЗІ 3.7-001-2005;
- розробка моделі загроз;
- розробка моделі порушника;
- розробка політики безпеки;
- синтез оптимальної КСЗІ;
- розробка документації на етапах впровадження і супроводу.

2. Розробка повинна бути представлена у вигляді моделі КСЗІ, працюючого програмного продукту для оцінювання рівня захисту, і супроводжуватись пояснювальною запискою, яка б містила в собі такі розділи:

- індивідуальне завдання на курсовий проект;
- аналіз структури підприємства та інформаційних потоків (розмежування доступу);
- категоріювання підприємства;
- дослідження середовищ функціонування ІТС підприємства;
- ідентифікацію загроз і моделі порушника;
- розробку моделі для оцінювання рівня захисту об'єкта захисту;
- розробку політики безпеки;
- розробку цільової функції для вибору механізмів та засобів захисту;
- синтез оптимальної КСЗІ;
- розробку відповідної документації на етапі впровадження і супроводу;
- висновки та перелік використаної літератури;
- додатки (технічне завдання; схема структурна підприємства; схема інформаційних потоків (матриця доступу); схема структурна КСЗІ підприємства; схема роботи програми).

Структура пояснювальної записки

Пояснювальна записка повинна відповідати індивідуальному завданню, а її оформлення – чинним стандартам, які слід враховувати на момент виконання розробки з врахуванням всіх офіційних змін, введених в дію.

Пояснювальна записка повинна мати таку структуру:

Вступна частина, яка містить:

- титульний аркуш;
- індивідуальне завдання;
- анотацію;
- зміст.

Основна частина, яка складається з:

- вступу;
- основної частини;
- висновків;
- списку використаних джерел.

Додатки, які розміщуються після основної частини пояснювальної записки курсового проекту, обов'язковими додатками є:

- Додаток А Технічне завдання;
- розроблені документи (акти, інструкції, плани тощо);

Графік виконання курсової роботи:

1-3 тижні – отримання завдання.

4-7 тижні – аналіз предметної області та літературних джерел згідно до обраної теми.

8-14 тижні – розробка звіту з аудиту інформаційної безпеки підприємства, розробка програмного забезпечення, що вирішує завдання курсової роботи, виконання розрахунків вартості КСЗІ для забезпечення необхідного рівня інформаційної безпеки.

15 тиждень – захист роботи. До захисту курсової роботи допускаються здобувачі, чия пояснювальна записка пройшла перевірку на плагіат та містить усі пункти, перелічені в даних методичних вказівках.

Критерії оцінювання курсової роботи

У цілому якісно виконана і захищена курсова робота оцінюється максимально у 100 балів. Семестрова робота над курсовою роботою оцінюється у 60 балів (0,6 кредиту), тобто по 30 балів у кожному семестровому модулі. Захист курсової роботи оцінюється у 40 балів (0,4 кредиту) за критеріями, наведеними у табл. 1.

Таблиця 1 – Критерії оцінювання захисту курсової роботи

№ з/п		Бали
1.	Якість оформлення курсової роботи (анотації, текстової частини, таблиць, рисунків, додатків, списку використаних джерел)	5
2.	Вміння здобувача презентувати результати роботи у доповіді на відкритому захисті (в повному обсязі висвітлені основні положення КР в логічній послідовності, наведені передумови та обґрунтовані розроблені пропозиції щодо удосконалення предмету КР, розроблена презентація)	10
3.	Відповіді здобувача на запитання комісії (здобувач володіє фаховою термінологією в рамках теми КР, вміє висловлювати та аргументувати власну думку, відповідь чітка, лаконічна, повна і вірна)	20
4.	Наявність апробації результатів курсової роботи (актів (довідок) на замовлення, про впровадження, публікацій (статей, тез доповідей) тощо)	5
Разом:		40

Критерії оцінювання семестровою роботи над курсовою роботою наведені в табл. 2.

Таблиця 2 – Критерії оцінювання курсової роботи

Тиждень	РН за ОП	Критерії оцінювання	Бали

1-7 тижні	RH5	При написанні Вступу КР зазначено її мету, задачі, предмет, об'єкт та інформаційні джерела. Вірно визначено і обґрунтовано у Вступі та першому теоретичному розділі роботи місце і значення об'єкту дослідження у сучасних системах захисту інформації.	10
	RH6	Проведено детальне дослідження обраної студентом області досліджень: знайдено найактуальніші оригінальні та оглядові статті, монографії, підручники, тощо. Зроблено обґрунтовані висновки стосовно стану дослідженої області та наявних в ній відкритих проблем.	10
	RH7	У першому розділі роботи розкрито сутність предмету дослідження КР та його роль і місце в практично використовуваних системах захисту інформації. Зроблені здобувачем власні висновки за матеріалами проведеного дослідження у теоретичному розділі.	10
8-13 тижні	RH24	Проведено теоретичні дослідження обраної проблеми. Висунуто гіпотези, твердження. Розроблено план необхідних експериментів для підтвердження отриманих теоретичних результатів. Зроблено висновки щодо очікуваних результатів експериментів.	6
	RH14	Створено необхідне програмне забезпечення для вирішення поставлених задач. Розроблене програмне забезпечення є сучасним, ефективним та здатним у повній мірі підтвердити або спростувати висновки теоретичного розділу.	8
	RH9	Проведені емпіричні дослідження, результати яких отримані та коректно представлені в курсовій роботі. Зроблено ґрунтовні висновки щодо підтвердження, спростування або уточнення отриманих в роботі теоретичних результатів.	10
	RH5	Представлено висновки по отриманим теоретичним та емпіричним результатам, виконано практичну імплементацію програмного продукту, що відображає отримані в роботі результати, або надано рекомендації щодо такої практичної імплементації. Зроблено висновки щодо можливих напрямків подальших досліджень.	6
Разом:			60

Виконання завдання

Рекомендації з організації Комплексної системи захисту інформації.

Дані рекомендації мають бути надані з урахуванням обмежень (технічних, фінансових тощо.). Бюджет (S) на проведення анкетування, аудиту, розробку рекомендацій та вибір програмного та технічного забезпечення КСЗІ рекомендовано *(не обов'язково робити це так)* вирахувати за наступною формулою:

$$S=(m+n)*1000 \text{ (доларів США),}$$

де m – число дати народження здобувача, n – місяць дати народження здобувача.

Перед виконанням завдання необхідно провести анкетування замовника КСЗІ.

Приклад набору категорій для анкетування наведено в таблиці 3.

Таблиця 3. Категорії для анкетування

№	Питання	Детальна інформація	Відповідь	
1	Інформація про замовника	Повна назва компанії Замовника		
		ПІБ особи, відповідальної за КСЗІ		
		Контактний номер телефону		
		Електронна адреса		
2	Визначення діяльності Замовника	Напрямок діяльності компанії		
		Наявність сумісних інформаційних ресурсів (інформаційного зв'язку) з іншими компаніями		
		Наявність філіалів компанії або віддалених офісів		
3	Характеристики приміщення, де розміщено автоматизовану систему	Наявність системи контролю доступу в приміщення або охорони		
		Наявність системи відеоспостереження		
		АС розміщено в одній будівлі		
		АС розміщено на одному поверсі		

		Наявність спеціальних приміщень (серверні чи комутаційні кімнати, архіви)		
4	Тип АС, що підлягають захисту, та їх кількість	АС1 (одна ЕВМ без доступу в інтернет та локальну мережу)		
		АС2 (локальна мережа без виходу в інтернет)		
		АС3 (корпоративна мережа з виходом в інтернет)		
		АС3 (веб-сайт або доступ до інформації через веб-додаток)		
5	Гриф доступу до інформації, що оброблюється в АС	Державна таємниця		
		Конфіденційна інформація, що є власністю держави		
		Конфіденційна інформація, що не є власністю держави		
		Персональні дані		
		Публічна інформація		
6	Користувачі АС, що мають доступ до інформації з обмеженим доступом	Загальна кількість		
		Поділ на групи		
		Права доступу до інформації		
		Наявність адміністратора безпеки чи системного адміністратора		
7	Технології обробки інформації з обмеженим доступом	Вказати як інформація імпортується/ експортується у/з системи		
		Місце зберігання		
		Спосіб обробки		
		Технологія резервування. архівування		
		Спосіб передачі		
		Спосіб захисту		
8	Представлення інформації, що зберігається	Текстові документи в ел. вигляді		
		Графічні документи в ел. вигляді		
		Електронний документообіг		
		БД		
		Спеціалізовані БД		
		ІР-телефонія		
		Відео-конференц зв'язок		
		Архіви/резервні копії в ел. вигляді		

		Паперова документація		
		Паперові архіви		
		Усна інформація		
9	Матриця прав доступу до інформації, що підлягає захисту	читання		
		внесення змін		
		копіювання		
		запис		
		видалення		
		Нагляд за каталогом		
10	Опис програмного забезпечення (ПЗ) в АС	Операційні системи (ОС) на робочих станціях		
		ОС на серверах		
		ОС на маршрутизаторах та ін. комунікаційному обладнанні		
		Спеціалізоване ПЗ на серверах		
		Спеціалізоване ПЗ на робочих станціях		
		Антивірусне ПЗ на серверах		
		Антивірусне ПЗ на робочих станціях		
		Програмний Firewall на серверах		
		Програмний Firewall на робочих станціях		
		Прикладне ПЗ		
11	Специфікація на апаратні та апаратно-програмні засоби АС	кількість серверів		
		кількість робочих станцій		
		склад та кількість маршрутизаторів та комутуючого обладнання		
		склад та кількість телекомунікаційного обладнання		
		типи з'єднань між компонентами мережі		
		опис засобів та технологій криптографічного захисту		
12	Опис та специфікація каналів зв'язку зі сторонніми організаціями	Типи каналів зв'язку:		
		локальна обчислювальна мережа		
		виділені канали		
		супутникові канали		
		бездротові мережі (WiMax,		

		WiFi, GPRS, CDMA)		
		мережі керування пристроями		
		Підключення до мережі Internet чи іншим зовнішнім каналам зв'язку:		
		провайдери		
		технології передачі даних		
		пропускна здатність		
13	Контактна інформація по анкеті	ПІБ особи, що заповнила анкету		
		Посада		
		Контактний телефон		

Оформлення пояснювальної записки

Анотація призначена для ознайомлення з текстовим документом курсового проекту. Анотація повинна коротко характеризувати мету роботи, засоби, використанні для досягнення поставленої задачі, коротку інформацію про досягнуті результати. Розмір анотації повинен становити приблизно 1/3 частину сторінки.

Анотація повинна бути двома мовами: українською та англійською. Анотацію розміщують безпосередньо за аркушем з індивідуальним завданням, починаючи з нової сторінки (третьої), нумерація якої не зазначається.

Зміст розташовують безпосередньо після анотації, починаючи з нової сторінки. До змісту включають: вступ; послідовно перелічені назви всіх розділів, підрозділів суті роботи; висновки; список використаних джерел; назви додатків і номери сторінок. Зміст не включає титульний лист, індивідуальне завдання на курсову роботу, анотацію та графічну частину. Нумерація у змісті починається зі Вступу (відповідно до нумерації у пояснювальній записці).

Сам зміст за нумерацією пояснювальної записки є четвертою сторінкою. Нумерація сторінок повинна бути наскрізною. Назви заголовків

змісту повинні однозначно відповідати назвам заголовків пояснювальної записки за текстом. Формування змісту у текстовому документі бажано формувати автоматично, використовуючи засоби обраного текстового редактора.

Вступ пишуть з нової пронумерованої сторінки з заголовком «ВСТУП» посередині великими літерами з більш високою насиченістю шрифту (напівжирний).

Текст вступу повинен бути коротким і висвітлювати питання актуальності, сучасного рішення, мети та завдання курсового проекту. У вступі і далі за текстом не дозволяється використовувати скорочені слова, терміни, крім загальноприйнятих.

Вступ висвітлює:

- стан розвитку проблеми в даній галузі, до якої має відношення розробка (важливість створення КСЗІ, забезпечення заданого рівня захисту тощо);
- актуальність, яка повинна подаватись в останньому абзаці вступу з метою стислого викладання суті обраної розробки;
- галузь використання та призначення даної розробки;
- мету та завдання.

Кількість сторінок вступу не повинна перевищувати 2 сторінки.

Проведення загального аналізу структури підприємства відбувається відповідно до НД ТЗІ 3.7-001-2005 і включає такі кроки:

1. Обстеження середовищ функціонування ІТС. Під час виконання цих робіт ІТС розглядається як організаційнотехнічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки (далі - середовища функціонування ІТС).

Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та

виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт. Обстеження виконується, коли розроблена концепція ІТС (основні принципи і підходи побудови), визначені основні завдання і характеристики ІТС, функціональних комплексів ІТС та існує варіант(и) їх реалізації.

При обстеженні обчислювальної системи ІТС повинні бути проаналізовані й описані:

- загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);

- види і характеристики каналів зв'язку;

- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;

- можливі обмеження щодо використання засобів та ін.

Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням та ін.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС (дані і програмне забезпечення).

Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, визначені й описані види (в термінах об'єктів КС) її представлення в ІТС.

Для кожного виду інформації і типу об'єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи КС (спостережність), яким вони повинні задовольняти.

Аналіз технології обробки інформації повинен виявити особливості обігу електронних документів, мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків.

Фіксуються види носіїв інформації та порядок їх використання під час функціонування ІТС. Для кожного структурного елемента схеми інформаційних потоків фіксуються склад інформаційних об'єктів, режим доступу до них, можливий вплив на нього (елементу) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

При обстеженні фізичного середовища здійснюється аналіз взаємного розміщення засобів обробки інформації ІТС на об'єктах інформаційної діяльності, комунікацій, систем життєзабезпечення і зв'язку, а також режим функціонування цих об'єктів.

Порядок проведення обстеження повинен відповідати ДСТУ 3396.1, а в частині, що стосується захисту інформації від витоку технічними каналами, - НД ТЗІ 3.1-001.

Аналізу підлягають такі характеристики фізичного середовища:

- територіальне розміщення компонентів ІТС (генеральний план, ситуаційний план);
- наявність охорони території та перепускний режим;

- наявність категорійованих приміщень, в яких мають розміщуватися компоненти ІТС;
- режим доступу до компонентів фізичного середовища ІТС;
- вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки;
- наявність елементів комунікацій, систем життєзабезпечення і зв'язку, що мають вихід за межі контрольованої зони;
- наявність та технічні характеристики систем заземлення;
- умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;
- наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

При обстеженні середовища користувачів здійснюється аналіз:

- функціонального та кількісного складу користувачів, їхніх функціональних обов'язків та рівня кваліфікації;
- повноважень користувачів щодо допуску до відомостей, які обробляються в ІТС, доступу до ІТС та її окремих компонентів; - повноважень користувачів щодо управління КСЗІ;
- рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІТС;
- наявності СЗІ в ІТС.

Результати обстеження середовищ функціонування ІТС оформлюються у вигляді акту і включаються, у разі необхідності, до відповідних розділів плану захисту інформації в ІТС (далі - План захисту), який розробляється згідно з НД ТЗІ 1.4-001.

За результатами обстеження середовищ функціонування ІТС затверджується перелік об'єктів захисту (з урахуванням рекомендацій НД ТЗІ 1.4-001, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010 щодо класифікації об'єктів), а також визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника.

Побудова моделей здійснюється відповідно до положень НД ТЗІ 1.1-002, НД ТЗІ 1.4- 001 та НД ТЗІ 1.6-003.

Модель загроз для інформації та модель порушника рекомендується оформляти у вигляді окремих документів (або поєднаних в один документ) Плану захисту. Наводиться структурна схема підприємства з указанням всіх відділів та працівників, які в них працюють, їх посади та функціональні обов'язки пов'язані з використанням інформаційних технологій та комп'ютерних мереж. Наводиться схема інформаційно-комунікаційної системи. Визначаються класи інформації за цілісністю, доступністю, конфіденційністю та спостережністю (табл. 2.2).

Таблиця 2.2 – Класифікація інформації.

Цілісність		Доступність		Конфіденційність	
Ц0	Критична	Д0	Критична	К0	Критична
Ц1	Дуже важлива	Д1	Дуже важлива	К1	Дуже важлива
Ц2	Важлива	Д2	Важлива	К2	Важлива
Ц3	Значима	Д3	Корисна	К3	Значима
Ц4	Не значна	Д4	Неістотна	К4	Мало значима

Аналізується характер інформаційних потоків між різними відділами та працівниками, виділяються інформаційні потоки, що потребують захисту, визначається статус інформації (комерційна таємниця, персональні дані, службова інформація, фінансова інформація, лише для внутрішнього використання, загальнодоступна тощо) (табл. 2.3).

Таблиця 2.3 – Інформація, що підлягає захисту

№	Вид	Ознаки КІ	Роль	Вид	Ресурс
1	Політика безпеки	Ц1, Д1, К0	Служба захисту інформації	Внутрішня	РС1, РС2

Як результат проведеного аналізу наводиться таблиця розмежування доступу для різних категорій працівників або відділів.

В підрозділі ідентифікація загроз, відповідно до структури об'єкта захисту повинні бути детально визначені загрози інформаційній безпеці.

Доцільно навести таблицю, в якій зазначити внутрішні і зовнішні загрози з ймовірностями їх виникнення.

У розділі розробки моделі оцінювання рівня захисту інформаційних ресурсів необхідно представити розроблену модель та результати її аналізу.

У розділі розробки політики безпеки навести відповідні правила 3-х рівневої політики безпеки. Наприклад:

- Забезпечення АВПЗ (антивірусне програмне забезпечення) (1-й рівень для найвищого керівництва);

- Використовувати ліцензійне АВПЗ; АВПЗ має бути встановлено на кожному робочому місті (2- рівень для середньої ланки, наприклад, керівник відділу);

- Використовувати Norton Antivirus; Оновлення антивірусних баз має відбуватися автоматично (3-й рівень, для безпосередніх виконавців);

Даний розділ має бути змістовним, конкретним, зрозумілим, оскільки саме він демонструє знання та навички у галузі аналізу безпеки підприємства. Рекомендований обсяг підрозділу – 4-7 сторінок пояснювальної записки.

У висновках до курсової роботи зазначити резюме за поточним станом інформаційної безпеки та дати рекомендації стосовно політики безпеки, якщо результати аудиту інформаційної безпеки вказують на таку необхідність.

Синтез оптимальної КСЗІ

Задачу синтезу комплексної системи захисту інформації сформулюємо як визначення оптимального складу комплексної системи захисту інформації. Для вирішення задачі побудови оптимальної структури комплексної системи захисту інформації для об'єкта захисту буде побудована цільова функція. В цільовій функції можуть враховуватись різні параметри, зокрема: N_{min} – мінімальний рівень надійності системи; P – ефективність захисту, C – вартість засобів захисту.

З урахуванням наведених параметрів цільова функція може мати вигляд:

$$\begin{cases} P \rightarrow \max \\ N \geq N_{\min} \\ C \leq C_0 \end{cases}$$

Відповідно до розробленої політики інформаційної безпеки потрібно обрати засоби захисту і розглянути варіанти їх можливих комбінацій. Вибір остаточного варіанту елементів і механізмів захисту виконується у відповідності до обмежень цільової функції.

Для створюваної КСЗІ можна обирати засоби та елементи КЗЗ, які ліцензовані на території України. Наприклад у таблиці 2.4 наведено можливі елементи захисту. Значення параметрів наведених механізмів захисту отримано експертним шляхом.

При викладенні тексту ПЗ забороняється переписування матеріалів літературних джерел, сканування рисунків, які мають відношення до основної частини. Частину описового матеріалу (у вигляді таблиць, рисунків, графічної інформації) бажано виносити у додатки до пояснювальної записки, а у тексті посилатись на ці додатки.

Якщо у курсовому проекті передбачається розробка програмного продукту, окремими підпунктами бажано описати розробку загальної схеми функціонування програми або схему роботи програми. Для окремих модулів, що входять до складу програмного засобу, необхідно розробити блок-схеми алгоритмів, структурні схеми з наведенням основних блоків, покрокове викладення алгоритму з розгалуженням і т. ін.

Наявність схем у пояснювальній записці є обов'язковою. Їх кількість і види повинні обиратися розробником таким чином, щоб вони допомагали зрозуміти роботу системи захисту в цілому і її складових. Всі схеми повинні бути виконані згідно з вимогами державних стандартів.

Таблиця 2.4 – Перелік засобів захисту

№	Назва засобу захисту	Надійність засобу	Ефективність захисту	Ціна, грн
С	Системи охоронної сигналізації			
1	Ajax GC-101 MINIKIT	0,5	0,6	1900
2	Tenex Guard 150GP	0,55	0,7	2300
3	Страж Avizor Kit	0,7	0,8	2600
4	Страж Evolution Kit	0,8	0,85	3100
КЗ	Детектори електромагнітного поля			
1	BH-03	0,5	0,6	400
2	BH-06	0,7	0,8	650
3	BugHunter Professional BH-02	0,9	0,9	3000
КВ	Камери відеоспостереження			
1	CDM-236SM	0,6	0,8	300
2	CDM-VF31S	0,7	0,8	400
3	CDM-332HQ-7	0,8	0,8	600
В	Відеореєстратори			
1	CHD-68EVH	0,8	-	800
2	CHD-116EVH	0,9	-	1200
3	ADM-816V 1.0	0,95	-	1800

Підрозділ повинен займати приблизно 8-10 сторінок ПЗ.

Забезпечення надійності КСЗІ на етапі проектування

Цей розділ повинен бути присвячений розробці структурної моделі КСЗІ та розрахунку заданих показників надійності. Цей розділ є практичної направленості і може містити до 3-х сторінок.

Висновки оформляють з нової пронумерованої сторінки посередині великими літерами більш високої насиченості. У висновках приводяться основні результати роботи над курсовим проектом. На основі результатів роботи надаються обґрунтовані висновки щодо переваг та недоліків застосування того чи іншого рішення. Наводяться недоліки та переваги

розробленої, труднощі при розробці та причини, що їх обумовили і можливі шляхи їх подолання, можливі рекомендації прикладного застосування та шляхами (перспективами) удосконалення розробленої захищеної мережі підприємства чи організації.

Список використаних джерел

Список містить перелік літературних джерел, на які повинні бути обов'язкові посилання в тексті пояснювальної записки. Література (книги, статті, патенти, журнали) в загальний список записується в порядку посилання на неї в тексті. В даному переліку дається оформлений відповідно до вимог ДСТУ ГОСТ 7.1:2006 «Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання», перелік літературних джерел, які було використано в процесі виконання проекту, і на яку є посилання в тексті пояснювальної записки. Кожне джерело повинно бути вказано разом з видавництвом, роком видання, кількістю сторінок. Літературу записують мовою оригіналу. В списку кожне джерело записують з абзацу, нумерують арабськими цифрами, починаючи з одиниці. Якщо у списку використаних джерел є посилання на Інтернет-сторінки,

слід наводити і їх. Приклад оформлення списку використаних джерел можна переглянути у списку використаних джерел у цих методичних вказівках.

Додатки

Обов'язковим додатком є технічне завдання (Додаток А). Технічне завдання розробляється студентом самостійно на основі індивідуального завдання протягом 2-х перших тижнів триместру. Інші додатки повинні містити матеріал, який не увійшов в основні розділи пояснювальної записки: план захисту, лістинг програм, структурна модель КСЗІ, результати моделювання КСЗІ, креслення, які займають більш ніж аркуш формату А4. При описі вказаних підпунктів рекомендується наводити безпосередньо по тексту або винести у додатки вигляд діалогових вікон, образи екранів і т.д., що пояснюють наведений текст. Кожен додаток необхідно починати з нової

сторінки, вказуючи зверху посередині рядка слово —Додаток‖ і через пропуск – його позначення. Додатки позначають послідовно великими українськими буквами, за винятком букв Г, Є, З, І, Ї, Й, О, Ч, Ъ, наприклад, Додаток А, Додаток Б і т.д. Якщо додатків більше ніж букв, то продовжують позначати арабськими цифрами. Дозволяється позначати додатки латинськими буквами, за винятком букв І і О. Кожен додаток повинен мати тематичний (змістовний) заголовок, який записують посередині рядка малими літерами . Сторінки додатків нумеруються, продовжуючи загальну нумерацію у пояснювальній записці. Всі додатки включають у зміст, вказуючи номер, заголовок і сторінки, з яких вони починаються. Приклад оформлення додатків можна переглянути у додатках до даних методичних вказівок.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Корченко О.Г., Гнатюк С.О., Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки: підручник. Київ : Національна академія СБУ, 2014. 189с.
2. В.О. Хорошко. Проектування комплексних систем захисту інформації. Видавництво Львівської політехніки, 2020. 317 с.
3. А.П.Курило, С.Л. Зефіров, В.Б. Голованов. Аудит информационной безопасности. – М. Издательская группа «БДЦ-Пресс», 2006. 304 с.
4. Н.В. Гришина. Организация КСЗИ. URL: <https://coollib.com/b/166590/read>
5. С.Е. Остапов, С.П. Євсєєв, О.Г. Король. Технології захисту інформації. Харків. Вид. ХНЕУ. 2013. 476 С.
6. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 28.12.2012 № 806). URL: <https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf>
7. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 15.10.2008 № 172). URL: <https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-005--99.pdf>
8. НД ТЗІ 2.6-001-2011 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, наказ Адміністрації Держспецзв'язку від 25.03.2011 № 65. URL: <https://tzi.com.ua/downloads/2.6-001-11.pdf>

9. НД ТЗІ 2.7-001-99 Технічний захист інформації в програмно-керованих АТС загального користування. Порядок виконання робіт, наказ ДСТСЗІ СБУ від 28.05.99 №26 (Зміна № 1 наказ від 28.12.2012 № 806). URL: <https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-2.7-001-99.pdf>

10. НД ТЗІ 2.7-009-2009 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, наказ Адміністрації Держспецзв'язку від 24.07.2009 № 172. URL: <https://tzi.com.ua/downloads/2.7-009-09.pdf>

11. НД ТЗІ 2.7-010-2009 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, наказ Адміністрації Держспецзв'язку від 24.07.2009 № 172. URL: <https://tzi.com.ua/downloads/2.7-010-09.pdf>

12. НД ТЗІ 2.7-011-2012 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв, наказ Адміністрації Держспецзв'язку від 23.07.2012 №389. URL: <https://tzi.com.ua/downloads/2.7-011-2012.pdf>

13. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу, наказ ДСТСЗІ СБ України від 20.12.2000 № 60. URL: http://www.dut.edu.ua/uploads/l_1036_36529430.pdf

14. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, наказ ДСТСЗІ СБ України від 08.11.2005 № 125. URL: <http://dndiime.org.ua/page/perelik-standartiv>

15. Серія стандартів ISO/IEC 27000 Інформаційні технології. Методи забезпечення безпеки. Менеджмент інформаційної безпеки. URL: <http://dndiime.org.ua/page/perelik-standartiv>

16. Указ Президента України №447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». URL: <https://www.president.gov.ua/documents/4472021-40013>

17. Закон України «Про основні засади забезпечення кібербезпеки України». URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

ДОДАТОК 1 Титульний лист

Міністерство освіти і науки України

Державний університет «Одеська політехніка»

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій

Кафедра кібербезпеки та програмного забезпечення

Петренко Іван Васильович,

студент групи XX-XXX

КУРСОВА РОБОТА МАГІСТРА

ТЕМА

Спеціальність:

125 Кібербезпека

Спеціалізація, освітня програма:

Управління кібербезпекою

Керівник:

Зоріло Вікторія Вікторівна,

ст. викладач

Одеса – 2022

ДОДАТОК 2 Завдання на курсову роботу

Міністерство освіти і науки України
Державний університет «Одеська політехніка»
Інститут інформаційної безпеки, радіоелектроніки та
телекомунікацій
Кафедра кібербезпеки та програмного забезпечення
Рівень вищої освіти другий (магістерський)
Спеціальність 125 – Кібербезпека
Освітня програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри КБПЗ

д.т.н., проф. А.А.Кобозєва
_____ 2022 р.

ЗАВДАННЯ НА КУРСОВУ РОБОТУ

Петренку Івану Васильовичу

1.Тема роботи:

керівник роботи *Зоріло Вікторія Вікторівна, ст. викладач*

2.Зміст роботи:

3. Перелік ілюстративного матеріалу:

4. Дата видачі завдання “ _____ ” _____ 20__ р.

ДОДАТОК 3 Календарний план

КАЛЕНДАРНИЙ ПЛАН

з/п	Назва етапів кваліфікаційної роботи	Строк виконання	При мітка
	<i>Перевірка на плагіат</i>		<i>виконано</i>

Здобувач вищої освіти _____

Петренко І.В.

Керівник роботи _____

Зоріло В. В.