МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»

Кафедра прикладної математики та інформатики

МЕТОДИЧНІ ВКАЗІВКИ
до виконання курсової роботи

з дисципліни «Архітектура програмних систем захисту інформації»

для студентів денної форми навчання
галузі знань 12 Інформаційні технології
спеціальності 125 Кібербезпека

Покровськ, 2022

УДК 004.056.5(072)

М 54

Методичні вказівки до виконання курсової роботи з дисципліни «Архітектура програмних систем захисту інформації» для студентів денної форми навчання галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека [Електронний ресурс] / уклад. Т.В. Алтухова. – Покровськ : ДВНЗ «ДонНТУ», 2022. – 20 с.

Методичні до виконання курсової роботи з дисципліни «Архітектура програмних систем захисту інформації» містять: завдання з варіантами, етапи для осмисленого виконання роботи студентами, основні вимоги до змісту пояснювальної записки і вимоги її оформлення та порядок оцінювання і захисту роботи. Завдання виконуються студентами у відповідності до заданого варіанту. В методичних вказівках наведено 30 варіантів.

Укладач: Алтухова Т. В., канд. техн. наук, доц. кафедри прикладної математики та інформатики ДВНЗ «ДонНТУ»

Рецензент: завідувач кафедри комп'ютерної інженерії ДВНЗ «ДонНТУ» , канд. техн. наук, доцент Ковальов С. О.

Відповідальний за випуск: Дмитрієва О. А., д-р техн. наук, проф., зав. кафедри прикладної математики та інформатики ДВНЗ «ДонНТУ»

Затверджено навчально-методичним відділом ДонНТУ,
протокол № 7 від 22.02.2022 р.

Розглянуто на засіданні кафедри прикладної математики та інформатики ДВНЗ «ДонНТУ» протокол № 2 від 22.02.2022 р.

ЗМІСТ

ВСТУП

За навчальним планом спеціальності 125 Кібербезпека дисципліна «Архітектура програмних систем захисту інформації» передбачає виконання курсової роботи за темою «Аналіз і дослідження архітектури програмної системи захисту інформації підприємства *(за предметною галуззю)*».

Курсова робота (КР) з даної дисципліни є самостійною роботою студента, що передбачає виконання завдань навчального, аналітично-розрахункового та науково-дослідницького характеру.

Мета виконання курсової роботи з дисципліни «Архітектура програмних систем захисту інформації» полягає у придбанні практичних навичок з проведення аналізу об’єктів захисту і вразливостей та розробки і дослідження політики інформаційної безпеки із застосуванням сучасних програмних систем захисту інформації відповідно до конкретної предметної області.

Основні компетентності та програні результати відповідно до ОПП Кібербезпека при вивченні дисципліни та виконання КР студентами [1]:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях;

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.);

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки;

ПРН01. Діяти на основі законодавчої, нормативно-правової баз України

та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та/або кібербезпеки;

ПРН12. Розробляти моделі загроз та порушника;

ПРН17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

ПРН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;

ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

Під час виконання КР студент повинен показати основні знання з правил побудови архітектури комплексних систем захисту інформації за умови аналізу основних показників інформаційної безпеки різноманітних підприємств, установ і організацій. Студент показує своє вміння здійснювати структурний аналіз предметної області та відповідних інформаційних потоків і вразливостей, розробляти на основі отриманих результатів моделі загроз та порушника, реалізовувати теоретичні дослідження з використанням відомих програмних систем формування політики інформаційної безпеки, розрахунку ризиків і захисту інформації.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ КУРСОВОЇ РОБОТИ

1.1 Завдання на курсову роботу

Індивідуальне завдання на курсову роботу за темою «Аналіз і дослідження архітектури програмної системи захисту інформації підприємства *(за предметною галуззю)*» визначається студентом у відповідності до запропонованого переліку (табл. 1) відповідно до списку групи або за двома останніми цифрами залікової книжки, таким чином, щоб у групі не здійснювалося повторення. Однак студент може запропонувати свою предметну галузь та узгодити з викладачем.

Таблиця 1 – Варіанти предметних областей

№	Предметна галузь	№	Предметна галузь
1	Вугледобувне підприємство	16	Інвестиційна компанія
2	Інформаційне агентство	17	Авіакомпанія
3	Хімічний завод	18	Проєктна організація
4	Електротехнічне підприємство	19	Підприємство з виробництва ювелірних прикрас
5	Транспортне підприємство (залізничний транспорт)	20	Підприємство з виробництва зброї
6	Підприємство з вироблення програмного забезпечення	21	Геологічне підприємство
7	Підприємство з виробництва будівельних матеріалів	22	Аптека
8	Фармацевтичний завод	23	Збагачувальна фабрика
9	Банківська установа	24	Приладобудівне підприємство
10	Вищий навчальний заклад (університет, інститут)	25	Шахтобудівне підприємство
11	Видавництво	26	Мобільні оператори
12	Підприємство нафтогазової промисловості	27	Туристична компанія
13	Конструкторське бюро	28	Електроенергетичне підприємство
14	Інтернет-провайдер	29	Суднобудівне підприємство
15	Інвестиційне підприємство	30	Машинобудівне підприємство

Для дослідження розроблених теоретичних положень виконується за допомогою програмного продукту Microsoft Security Assessment Tool з формування політики інформаційної безпеки, розрахунку ризиків і захисту інформації (методологія MSAT).

1.2 Етапи виконання

В процесі виконання курсової роботи з дисципліни «Архітектура програмних систем захисту інформації» передбачається виконання на ступних етапів роботи:

1. Виконується ознайомлення з тематикою курсової роботи та визначення предметної галузі для формування політики інформаційної безпеки.
2. Виконується теоретичне дослідження нормативно-правових аспектів захисту інформації та відповідної обраної предметної галузі. Дане дослідження передбачає виконання наступних пунктів:
   - аналіз нормативно-правової основи з інформаційного захисту;
   - аналіз структури предметної галузі та її інформаційні потоки;
   - аналіз можливих вразливостей інформаційної безпеки предметної галузі;
   - розробка моделей загроз та порушника відповідно до отриманих результатів аналізу предметної галузі.
3. Виконується опис методології MSAT, що використовується для формування політики інформаційної безпеки, розрахунку ризиків і захисту інформації, та порівняльний аналіз з іншими відомими методологіями.
4. Виконується експериментальний аналіз отриманих результатів теоретичного дослідження за предметною галуззю за допомогою програмного продукту Microsoft Security Assessment Tool.

2. ОСНОВНІ ВИМОГИ ДО ЗМІСТУ КУРСОВОЇ РОБОТИ ТА ПРАВИЛА ОФОРМЛЕННЯ ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

2.1 Вимоги до змістовної структури та обсягу пояснювальної записки

Курсова робота з дисципліни «Архітектура програмних систем захисту інформації» повинна містити наступні елементи:

1. Титульний лист (додаток А «Титульний аркуш»)

2. Технічне завдання (додаток Б «Приклад технічного завдання»)

3. Анотація (додаток В «Анотація»)

Анотація призначена для ознайомлення з основними змістом і положенням виконаної роботи в курсовій. В анотації необхідно надати коротку інформацію щодо мети і завдань курсової роботи; засобів, що застосовуються для досягнення поставленого завдання, та досягнути в процесі її виконання результатів. Загальний її розмір повинен становити приблизно 1/3 сторінки та містити ключові слова.

4. Зміст ***(1-2 сторінки)***

У ***змісті*** відображуються основні розділи та підрозділи пояснювальної записки з відповідними номерами сторінок, де вони розташовуються.

5. Вступ ***(2-3 сторінки)***

У ***Вступі*** необхідно висвітлити актуальність загальної проблеми інформаційної безпеки та питань сучасного стану з формування політики інформаційної безпеки, розрахунку ризиків і захисту інформації, виконується обґрунтування необхідності вирішення проблеми, можливі шляхи реалізації. Формується головна мета курсової роботи та основні завдання з її вирішення, а також наводяться вихідні дані курсової роботи.

6. Теоретична частина ***(15-20 сторінок)***

Теоретична частина передбачає виконання теоретичного дослідження з нормативно-правових засад інформаційної безпеки та самого об’єкту

захисту відповідно до вимог НД ТЗІ 3.7-001-2005, його існуючих інформаційних потоків і вразливостей інформаційної безпеки; розробку моделей загроз і порушника за отриманими результатами дослідження об’єкту захисту.

7. Практична частина ***(10-15 сторінок)***

Практична частина повинна містити опис застосовуваної методології MSAT для формування політики інформаційної безпеки, розрахунку ризиків і захисту інформації; порівняльний аналіз з іншими відомими методологіями з визначенням її переваг і недоліків; експериментальний аналіз ризиків порушення захищеності інформаційних систем за обраною предметною галуззю та результатами проведених теоретичних досліджень.

8. Висновки ***(1-2 сторінки)***

У ***Висновках*** наводяться отримані результати під час виконання курсової роботи та можливі шляхи і рекомендації подолання існуючих ризиків інформаційної безпеки задля удосконалення більш ефективного захисту підприємства, установи чи організації, що розглядалися.

9. Список використаних джерел

У ***Списку використаних джерел*** наводиться *15-20* посилань. Оформлення списку використаних джерел виконується згідно ДСТУ ГОСТ 7.1:2006 «Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання» [2].

10. Додатки *(за наявності)*.

Пояснювальна записка курсової роботи передбачає загальний обсяг приблизно **30-40** сторінок, які друкуються на одній стороні аркуша.

.

2.2 Правила оформлення пояснювальної записки

Курсова робота виконується лише державною мовою, без орфографічних та синтаксичних помилок. Весь текст повинен бути логічно

викладений, перехід з одного пункту до іншого забезпечується тільки після логічного завершення.

Весь запозичений текст з літературних джерел інформації повинен мати посилання по тексту.

Пояснювальна записка оформлюється наступним чином:

- формат – А4 (друк виконується лише з однієї сторони);
- поля: зліва – 25 мм; справа – 15 мм; зверху та знизу – 20 мм;
- шрифт – Times New Roman;
- розмір – 14;
- абзац – 1,25 см;
- міжрядковий інтервал – 1,5.

Кожний ***розділ*** курсової роботи починається з нового аркушу, в якому є логічні частини – підрозділи. Нумерування розділу виконується арабськими цифрами, наприклад «1» (перший розділ), а підрозділу здійснюється згідно порядкового номеру розділу та самого підрозділу, наприклад «1.1» (перший підрозділ першого розділу.

Всі заголовки основних елементів наводяться великими літерами та посередині без відступів, наприклад «ЗМІСТ», «ВСТУП», «РОЗДІЛ», «ВИСНОВКИ», «СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ», в яких наприкінці крапка не ставиться. Підрозділи друкуються звичайними літерами з рівнянням по ширині з відступом, наприклад «1.1 Аналіз нормативно-правових засад інформаційної безпеки» та крапка наприкінці також не ставиться. Відстані між заголовками розділів і підрозділів та підрозділами і основним текстом – 2 рядки. Розміщення заголовків елементів пояснювальної записки у нижній частині без хоча б одного рядка тексту забороняється.

Нумерація сторінок виконується у верхньому куті аркуша справа арабськими цифрами, титульний аркуш не нумерується, проте входить до кількості сторінок пояснювальної сторінки.

Наведення таблиць у тексті

Таблиці, в яких наведено матеріал тексту, повинні мати назву та

порядковий номер, який ставиться у відповідності до розділу, де вона наводиться. Розміщення таблиці виконується безпосередньо після посилання на неї, наприклад, «наведено в табл. 2.1» (перша таблиця другого розділу), та бажано на одному аркуші, проте у випадку, коли частина її переноситься на інший аркуш, то виконується розрив таблиці та у правому верхньому куті наводиться «Продовження таблиці 2.1 –». Заголовки таблиці повинні бути як у основній частині, так і при перенесенні її на іншу сторінку.

Таблиця 2.1 – Назва таблиці

Заголовки рядків	Заголовки	
	підзаголовки	підзаголовки
Рядки	Текст	Текст
Рядки	Текст	Текст

Рисунок 2.1 – Зразок оформлення таблиці

Наведення ілюстрацій в тексті

Під час оформлення пояснювальної записки виникає необхідність наведення ілюстрацій (схеми, графіки, графічні зображення, тощо) у тексті. Вони розміщуються безпосередньо після згадування у тексті вперше, наприклад «наведено на рис. 1.1» або «див. рис. 1.1», або на наступній сторінці. Розміщення ілюстрації виконується по центру без виступів та позначається наступним чином «Рисунок 1.1 – Принципова схема інформаційних потоків при формуванні системи керування безпекою супермаркету» (Номер рисунка та його назва розміщуються під рисунком).

Надання в тексті формул та посилань

Наведення формул в пояснювальній записці виконується в межах розділу та нумерація виконується арабськими цифрами, наприклад (2.1) (перша формула другого розділу). Розташування формули виконується посередині без відступів та мають пробіл до та після виразу. Пояснення елементів формули здійснюється безпосередньо під формулою в тій послідовності, в якій їх наведено у виразі, та починається з нового рядка для кожного символу або коефіцієнту.

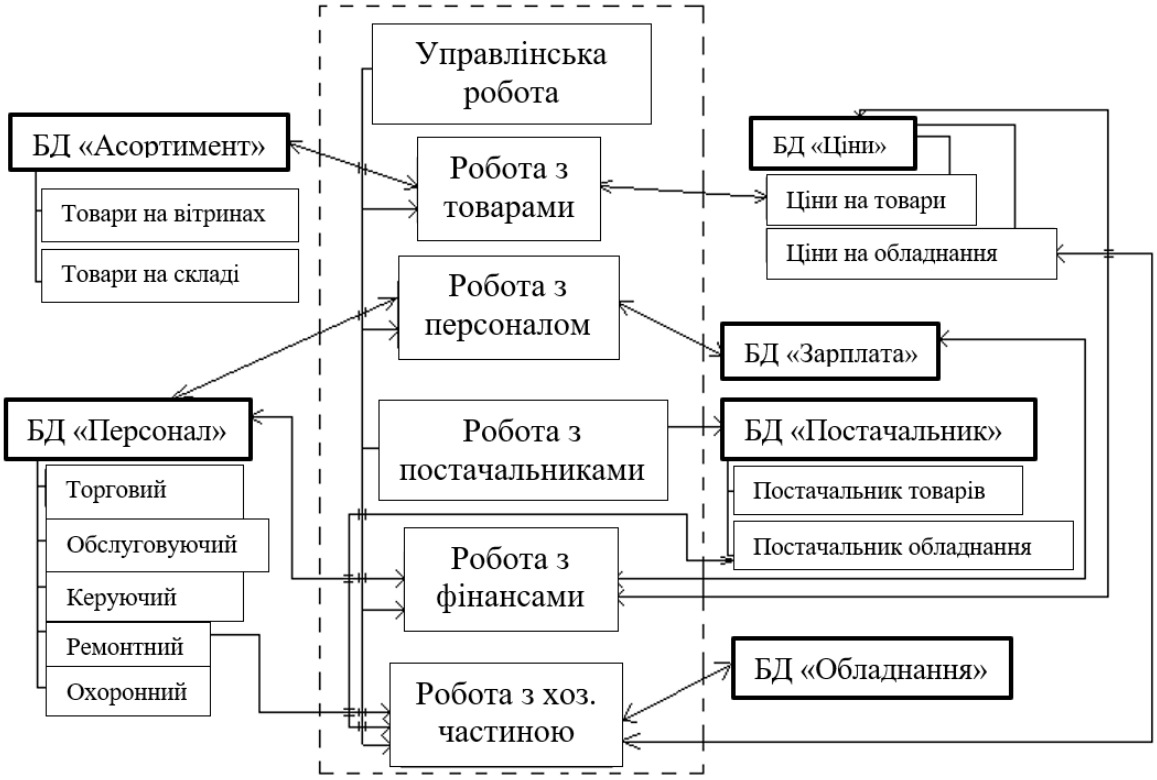

Рисунок 1.1 – Принципова схема інформаційних потоків при формуванні системи керування безпекою супермаркету

Рисунок 2.2 – Зразок оформлення ілюстрації

В тексті пояснювальної записки при запозиченні інформації необхідно наводити посилання на джерело інформації, наприклад «[1]» або «[1, стор. 12]». Цитування тексту виконується у лапках, і наводиться у тому ж контексті, що і у джерелі інформації та супроводжується обов’язковим посиланням.

3. ПОРЯДОК ОЦІНЮВАННЯ ТА ЗАХИСТУ КУРСОВОЇ РОБОТИ З ДИСЦИПЛІНИ

3.1 Критерії оцінювання результатів виконання курсової роботи з дисципліни

Оцінювання результатів виконання курсової роботи виконується за 100-бальною шкалою:

Критерії оцінювання курсової роботи

Пояснювальна записка		Захист	Максимальний бал
Теоретична частина	Практична частина		
25	15	60	100

«відмінно» (90-100 балів) – під час виконання курсової роботи студент вчасно виконував всі поставленні завдання на високому рівні; проявляв творчий підхід до виконання досліджень у відповідності до обраної предметної галузі; своєчасно надав на кафедру пояснювальну записку у друкованому і електронному варіанті, оформлену згідно вимог, та отримав високі позитивні бали під час захисту курсової роботи;

«добре» (74-89 балів) – під час виконання курсової роботи студент вчасно виконував всі поставленні завдання на достатньому рівні; проявляв знання на достатньому рівні при виконанні досліджень та допустив незначні помилки при їх виконанні; своєчасно надав на кафедру пояснювальну записку у друкованому і електронному варіанті і отримав незначні зауваження щодо оформлення згідно наданих вимог та позитивні бали під час захисту курсової роботи;

«задовільно» (60-73 балів) – під час виконання курсової роботи студент виконував поставленні завдання та допускав значні помилки; недостатньо застосовував знання з проведених досліджень в галузі інформаційної безпеки; при виконанні аналізу самої роботи не надав увагу своїм помилкам та недолікам; при виконанні оформлення пояснювальної записки було не

вирішено в достатньому обсязі поставлені завдання або були неточності чи логічні помилки та отримав загалом позитивну оцінку при захисту курсової роботи;

«незадовільно» (30-59 балів) – студент не регулярно виконував поставленні завдання та допускав досить серйозні помилки під час їх виконання; при виконання курсової роботи не показав задовільний рівень знань для проведення досліджень; під час оформлення пояснювальної записки було допущено низку серйозних помилок і не вирішено певні поставлені завдання, що повинні бути наведені в роботі, тобто відсутні окремі розділи чи підрозділи курсової роботи.

3.2 Захист курсової роботи

При отриманні позитивної оцінки пояснювальної записки від керівника та своєчасного її надання на кафедру студент допускається до захисту курсової роботи. Захист курсової роботи здійснюється у термін, що встановлюється згідно Положення про семестровий контроль у ДВНЗ «Донецький національний технічний університет» [3], за участі комісії у складі керівника курсової роботи та одного чи двох викладачів кафедри. Для студентів денної форми навчання захист курсової роботи не виноситься у розклад занять, а для заочної форми навчання передбачається внесення до розкладу заліково-екзаменаційної сесії.

На захист виносяться основні положення курсової роботи та студентом готується виступ, що супроводжується презентацією. Виступ студента не повинен тривати більше 7-10 хвилин, після якого комісія може задати питання щодо більш чіткого уявлення та уточнення окремих положень виступу і виконаної курсової роботи. Кінцевий результат оцінюється згідно описаним вище критеріям (п. 3.1).

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Освітньо-професійна програма «Кібербезпека» [Електронний ресурс]. – Режим доступу : https://wiki.donntu.edu.ua/images/8/84/%D0%9E%D0%9F%D0%9F_%D0%9A%D0%86%D0%91_%28%D0%B1%D0%B0%D0%BA%29_2020.pdf. – Назва з екрана.

2. ДСТУ ГОСТ 7.1:2006 «Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання» [Електронний ресурс]. – Режим доступу : https://dnaop.com/html/33995/doc-%D0%94%D0%A1%D0%A2%D0%A3_%D0%93%D0%9E%D0%A1%D0%A2_7.1_2006. – Назва з екрана.

3. Положення про семестровий контроль у ДВНЗ «Донецький національний технічний університет» [Електронний ресурс]. – Режим доступу : https://donntu.edu.ua/wp-content/uploads/2021/01/2020-12-28-%D0%9F%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F-%D0%BF%D1%80%D0%BE-%D1%81%D0%B5%D0%BC%D0%B5%D1%81%D1%82%D1%80%D0%BE%D0%B2%D0%B8%D0%B9-%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C-%D0%94%D0%BE%D0%BD%D0%9D%D0%A2%D0%A3-2020-%D0%9C%D0%9F.pdf. – Назва з екрана.

4. Лужецький, В.А. Основи інформаційної безпеки : навч. посіб. [рек. МОН] / В.А. Лужецький, О.П. Войтович, В.Д. Кожухівський. – Вінниця : ВНТУ, 2013. – 246 с.

5. Інформаційна безпека цифрових програмно-керованих АТС : навч. посіб. / С.М. Горохов, В.Г. Кононович, С.В. Стайкуца та ін. – Одеса : ОНАЗ ім. О.С. Попова, 2013. – 244 с.

6. Гребенніков, В.В. Комплексні системи захисту інформації :

проектування, впровадження, супровід / В.В. Гребенніков. – Litres, 2019. – 613 с.

7. Проєктування комплексних систем захисту інформації : підручник / В.О. Хорошко, І.М. Павлов, Ю.Я. Бобало та ін. – Львів : Вид-во Львів. політехніки, 2020. – 320 с.

8. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. / В.М. Богуш, В.В. Богуш, В.Д. Бровко, В.П. Настрадін. – К. : Ліра-К, 2020. – 554 с.

9. Про інформацію : Закон України поточна редакція від 16.07.2020 р. №2657-XII [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2657-12#Text. – Назва з екрана.

10. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України поточна редакція від 04.07.2020 р. №80/94-ВР [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text. – Назва з екрана.

11. НД ТЗІ 3.7-003-05. Порядок проведення робіт зі створення КСЗІ [Електронний ресурс]. – Режим доступу : https://tzi.com.ua/downloads/3.7-003-2005.pdf. – Назва з екрана.

ДОДАТОК А «*Титульний аркуш*»

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»
Кафедра прикладної математики та інформатики

КУРСОВА РОБОТА

з дисципліни: **Архітектура програмних систем захисту інформації**

на тему: **«Аналіз і дослідження архітектури програмної системи захисту інформації підприємства *(за предметною галуззю)*»**

Виконав студент __ курсу групи _____
Спеціальності **125 Кібербезпека**
Ім'я ПРІЗВИЩЕ _____
(підпис)

«__» _____ 2022 р.

Перевірив: _____
(вчений ступінь, вчений звання, посада)

Ім'я ПРІЗВИЩЕ _____
(підпис)

Кількість балів:
Пояснювальна записка:
Теоретична частина _____
(кіл-ть балів)

Практична частина _____
(кіл-ть балів)

Захист курсової роботи _____
(кіл-ть балів)

Оцінка за національною шкалою: _____
(відм., добре, задов./кіл-ть балів)

Члени комісії _____ _____
(підпис) *(прізвище та ініціали)*

_____ _____
(підпис) *(прізвище та ініціали)*

Покровськ, 2022

ДОДАТОК Б «*Приклад технічного завдання*»

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»

Факультет: комп'ютерно-інтегрованих технологій та автоматизації
Кафедра: прикладної математики та інформатики
Дисципліна: Архітектура програмних систем захисту інформації
Спеціальність: 125 Кібербезпека
Курс: ____ **Група:** _____ **Семестр:** ___

ТЕХНІЧНЕ ЗАВДАННЯ

на курсову роботу студента

Ім'я ПРІЗВИЩЕ

1. Тема курсової роботи: **Аналіз і дослідження архітектури програмної системи захисту інформації підприємства *(за предметною галуззю)***
2. Термін здачі студентом закінченої роботи **_____20__ р.**
3. Вихідні дані для виконання курсової роботи **Предметна галузь, методологія MSAT**
4. Зміст пояснювальної записки (перелік питань, що підлягають розгляду):
   1. Теоретична частина
   - аналіз нормативно-правових засад з інформаційного захисту;
   - аналіз структури предметної галузі та її інформаційні потоки;
   - аналіз можливих вразливостей інформаційної безпеки предметної галузі;
   - розробка моделей загроз та порушника відповідно до отриманих результатів аналізу предметної галузі.

   2. Практична частина
   - опис методології MSAT, що використовується для формування політики інформаційної безпеки, розрахунку ризиків і захисту інформації;
   - порівняльний аналіз методології MSAT з відомими методологіями забезпечення інформаційного захисту;
   - експериментальний аналіз отриманих результатів теоретичного дослідження за предметною галуззю за допомогою програмного продукту Microsoft Security Assessment Tool.

5. Дата видачі завдання _____

Календарний план виконання курсової роботи

№ п/п	Назва етапів курсової роботи	Термін виконання етапів роботи	
		початок	закінчення
1	Теоретична частина		
1.1	Аналіз нормативно-правових засад з інформаційного захисту		
1.2	Аналіз структури предметної галузі та її інформаційні потоки		
1.3	Аналіз можливих вразливостей інформаційної безпеки предметної галузі		
1.4	Розробка моделі загроз		
1.5	Розробка моделі порушника		
2	Практична частина		
2.1	Опис методології MSAT		
2.2	Порівняльний аналіз методології MSAT з відомими методологіями забезпечення інформаційного захисту		
2.3	Експериментальний аналіз отриманих результатів теоретичного дослідження за предметною галуззю за допомогою програмного продукту Microsoft Security Assessment Tool		
	Оформлення курсової роботи		
	Подання на перевірку		
	Захист роботи		

Студент _____ Ім’я ПРИЗВИЩЕ

Керівник курсової роботи _____ Ім’я ПРИЗВИЩЕ

Дата видачі завдання «_____»_____20__ р.

ДОДАТОК В «*Анотація*»

АНОТАЦІЯ

Ім'я ПРІЗВИЩЕ. Аналіз і дослідження архітектури програмної системи захисту інформації підприємства *(за предметною галуззю)*/ Курсова робота з дисципліни «Архітектура програмних систем захисту інформації», спеціальність 125 Кібербезпека. – ДВНЗ «ДонНТУ», Покровськ, 2022.

Текст ….
Текст ….
Текст ….
Текст ….
Текст ….
Текст ….
Текст ….
Текст ….
Текст ….
Текст ….
Текст ….

Ключові слова: 5-7 слів