Методичні вказівки
до виконання курсових робіт з дисципліни «Проєктування систем кібербезпеки» зі спеціальності «Кібербезпека та захист інформації» (освітня програма «Безпека інформаційних і комунікаційних систем»)

Міністерство освіти і науки України
Вінницький національний технічний університет

Методичні вказівки до виконання курсових робіт з дисципліни «Проєктування систем кібербезпеки» зі спеціальності «Кібербезпека та захист інформації» (освітня програма «Безпека інформаційних і комунікаційних систем»)

Вінниця
ВНТУ
2025

Рекомендовано до видання Радою з якості освіти Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 9 від 17.04.2025 р.)

Рецензенти:
В. А. Майданюк, кандидат технічних наук, доцент
О. П. Войтович, кандидат технічних наук, доцент
Д. Х. Штофель, кандидат технічних наук, доцент

Методичні вказівки до виконання курсових робіт з дисципліни «Проєктування систем кібербезпеки» зі спеціальності «Кібербезпека та захист інформації» (освітня програма «Безпека інформаційних і комунікаційних систем») [Електронний ресурс] / уклад. Л. М. Куперштейн. – Вінниця : ВНТУ, 2025. – (PDF, 49 с.)

Методичні вказівки призначені для надання допомоги при виконанні курсових робіт з дисципліни «Проєктування систем кібербезпеки» і оформленні пояснювальної записки до неї. Наведено перелік можливих тем для розробки, сформульовано вимоги до програмного засобу, що реалізуватиме основну мету роботи, дано рекомендації щодо коректного оформлення пояснювальної записки, наведено критерії оцінювання курсової роботи.

ЗМІСТ

1 ТЕМАТИКА ТА ЗМІСТ КУРСОВОЇ РОБОТИ

1.1 Тематика

Курсова робота (КР) – навчальна самостійна робота з дисципліни, яка містить елементи (задачі) навчального, аналітично-розрахункового та науково-дослідницького характеру.

В курсовій роботі з дисципліни «Проєктування систем кібербезпеки» студент має показати знання основних принципів проєктування та подальшого практичного застосування систем захисту інформації та асоційованих із ними програмних засобів.

Студент має вміти проєктувати систему захисту інформації, що полягає у виконанні передпроєктного аналізу предметної області системи захисту, формулюванні вимог до проєктованої системи та розробки технічного завдання, розробці технічного та робочого проєкту системи захисту, оформленні програмної та експлуатаційної документації на проєкт, тестуванні програмної системи захисту, оцінюванні ефективності розробленої системи.

Тематика курсової роботи пов’язана з майбутньою спеціальністю студентів. Для програмної реалізації даної курсової роботи пропонується розробка системи захисту інформації в кіберпросторі або асоційованих із цією тематикою програмних чи програмно-апаратних засобів.

Під час виконання курсової роботи студенти мають використати всі знання, отримані ними під час вивчення дисциплін «Проєктування систем кібербезпеки», «Кібербезпека».

Зміст курсової роботи відповідає програмі дисципліни і повинен відображати суть теми, яка розглядається.

Зміст курсової роботи визначається індивідуальним завданням, яке видається викладачем кожному студенту. Завдання видається не пізніше другого тижня семестру, в якому виконується КР. Курсове проєктування включає декілька послідовних етапів, які, в загальному випадку, пов'язані із змістовною постановкою задачі, розробкою індивідуального завдання та технічного завдання, вибором форми представлення задачі, передпроєктним аналізом системи захисту, техноробоче проєктування, тестування та оцінку ефективності запропонованої системи результатів. Кожен етап роботи обов’язково має знайти своє відображення в пояснювальній записці, що містить вихідні та розрахунково-пояснювальні матеріали, які пов'язані з виконанням курсової роботи.

Завдання для курсових робіт визначаються викладачем із загального списку завдань на курсову роботу. Заохочуються пропозиції студентів щодо самостійного, за узгодженням з викладачем, вибору теми курсової роботи поза межами запропонованого в методичних вказівках переліку. Самостійний вибір предметної області, в якій доцільно використовувати сучасні методи захисту систем та оригінальні алгоритми, дозволяє зробити висновок

щодо рівня творчої активності студента, його вміння самостійно здійснити попередній аналіз предметної області і розробити технічне завдання.

Метою індивідуальних завдань є закріплення теоретичних та практичних навичок в роботі з використання сучасних методів та засобів захисту інформації в комп'ютерних системах та мережах.

В 2 семестрі здобувачам вищої освіти пропонується виконати курсову роботу (КР – 45 год/1,5 кредиту). Завдання на курсову роботу включає весь матеріал, який було опрацьовано під час лекційних, практичних, лабораторних та самостійних занять протягом курсу вивчення дисципліни.

1.2 Об'єм курсової роботи та її зміст

Обсяг основної частини курсової роботи повинен складати 25-30 сторінок.

При виконанні курсової роботи обов'язково повинні бути використані такі елементи:

- передпроєктний аналіз предметної області системи;
- техноробоче проєктування системи захисту;
- тестування та оцінка ефективності системи захисту.

Розробка повинна бути представлена у вигляді готового працюючого програмного, програмно-апаратного, апаратного засобу, системи або методики і супроводжуватись пояснювальною запискою, яка б містила в собі такі розділи:

- індивідуальне завдання на курсову роботу;
- передпроєктний аналіз системи захисту;
- техноробоче проєктування системи захисту;
- впровадження системи захисту;
- висновки та перелік використаних джерел;
- додатки;
- технічне завдання;
- схема алгоритму програми/засобу;
- схема структурна засобу;
- текст програми;
- програма та методика випробувань;
- керівництво користувача (оператора/адміністратора);
- ілюстративна частина.

2 ОФОРМЛЕННЯ ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

2.1 Загальні правила оформлення

При оформленні пояснювальної записки потрібно дотримуватись вимог до оформлення курсових робіт згідно «Положення про курсове проєктування в ВНТУ» (затверджено наказом ВНТУ № 275 від 29.08.2024 р.). Текст пояснювальної записки повинен бути набраний на комп'ютері та роздрукований на принтері. В університеті діє процедура електронного прийняття та передачі в архів пояснювальних записок курсових робіт в електронному вигляді, тому роздруковувати пояснювальну записку не потрібно.

Обсяг. Обсяг текстової частини визначається кількістю годин СРС, які виділяються для дисципліни на курсову роботу навчальним планом (25−30 с.).

Шрифт і поля. Текст ПЗ виконується у відповідності з вимогами «Положення про курсове проєктування в ВНТУ». Текст набирають шрифтом Times New Roman чорного кольору прямого накреслення через півтора міжрядкові інтервали, кегль (розмір шрифту) 14. Кегль шрифту може бути зменшений в таблицях, у написах на рисунка, у додатках, але не у їх назвах.

Поля аркушів КР/КП встановлюють такої ширини: верхнє та нижнє – по 20 мм, ліве – 25 мм, праве – 10 мм.

Нумерація сторінок. Сторінки повинні бути пронумеровані, починаючи з другої (анотації) після титульного аркушу, при цьому індивідуальне завдання нумерується. Номер сторінки вказується у правому верхньому кутку сторінки. Нумерація додатків продовжує основну нумерацію.

Оформлення розділів і підрозділів. Структурними елементами основної частини ПЗ є розділи, підрозділи, пункти, підпункти, переліки.

Крім того є такі складові ПЗ як титульна сторінка, анотація, зміст, вступ, висновки, список використаних джерел та додатки. Ці складові мають заголовок першого рівня, який на відміну від основної частини виконується з вирівнюванням по центру великими літерами.

Розділ – головна ступінь поділу тексту, позначена номером і має заголовок першого рівня. *Підрозділ* – частина розділу, позначена номером і має заголовок другого рівня. *Пункт* – частина розділу чи підрозділу, позначена номером і може мати заголовок третього рівня. Заголовки структурних елементів потрібно нумерувати тільки арабськими числами.

Кожен розділ рекомендується починати з нової сторінки. Заголовок розділу записують з абзацу великими літерами, після заголовку до тексту або підзаголовку пропускають один рядок. Заголовки розділів, підрозділів та пунктів (при наявності заголовка) записують з абзацу малими літерами, починаючи з великої. Перед заголовком розділу і після нього пропускають один рядок. Перед та після заголовку підрозділу пропускається один рядок.

Розділи нумерують порядковими номерами в межах всього документа

(1, 2 тощо). Підрозділи нумерують в межах кожного розділу, пункти – в межах підрозділу за формою (3.1, 3.2, 3.2.1, 3.2.2 тощо). Цифри, які вказують номер, не повинні виступати за абзац. Після номера крапку не ставлять, а пропускають один знак.

Заголовки розділів і підрозділів, пунктів і підпунктів не повинні містити знаків переносу на новий рядок. Назви розділів і підрозділів, пунктів і підпунктів не повинні мати крапки в кінці.

Допускається розміщувати текст між заголовками розділу і підрозділу, між заголовками підрозділу і пункту. Посилання в тексті на розділи виконується за формою: «...наведено в розділі 3».

Оформлення таблиць. Таблицю розміщують симетрично до тексту після першого посилання на даній сторінці або на наступній, якщо на даній вона не уміщується і таким чином, щоб зручно було її розглядати без повороту або з поворотом на кут 90°. Таблиці у тексті пояснювальної записки набираються основним шрифтом, в деяких випадках розмір шрифту може бути зменшений до 10-12 пт. Підписи таблиць розташовуються над таблицею з вказанням її номеру і назви, вирівнявши по лівому краю таблиці. Приклад наведено у табл.2.1.

Таблиця 2.1 - Мережеве обладнання

№	Обладнання	Назва	IP-адреса	MAC-адреса
1	Сервер	Server	192.168.6.2/24	D01E.64B5.30D1
3	Комутатор	switch1	-	-

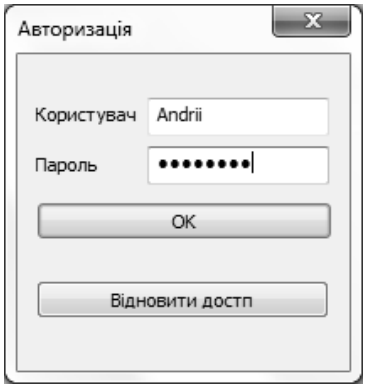
На всі таблиці мають бути посилання за формою «... в табл. 2.1» або в дужках по тексту (табл. 2.1). Посилання на раніше наведену таблицю дають із скороченим словом «дивись» (див. табл. 2.4) за ходом чи в кінці речення.

При перенесенні частин таблиці на інші сторінки, повторюють або продовжують найменування граф. Допускається виконувати нумерацію граф на початку таблиці і, при перенесенні частин таблиці на наступні сторінки, повторювати тільки нумерацію граф. У всіх випадках назва таблиці розміщується тільки над першою частиною, а над іншими частинами зліва пишуть «Продовження таблиці 1.1» без крапки в кінці.

Бажано використовувати засоби автоматичної нумерації пунктів.

Оформлення рисунків. Розміщують рисунки в тексті або в додатках. В тексті рисунки розміщують симетрично до тексту після першого посилання на них або на наступній сторінці, якщо на даній вони не уміщуються без повороту. На всі рисунки мають бути посилання за формою: «... на рис. 3.5», або в дужках по тексту (рис. 3.6). Посилання на раніше наведений рисунок дають із скороченням (див. рис. 1.4).

Кожен рисунок повинен мати номер і підпис, розташовані під рисунком по центру. Крапку в кінці не ставлять, знак переносу не використовують.



Якщо найменування рисунка довге, то його продовжують у наступному рядку, починаючи від найменування. Приклад показано на рис. 2.1.

Рисунок 2.1 – Вигляд вікна авторизації

Між рисунком і текстом пропускають один рядок. Нумерують рисунки в межах розділів або в межах всього документа.

Бажано використовувати засоби автоматичної нумерації рисунків.

Оформлення переліків. Переліки, за потреби, можуть бути наведені в тексті ПЗ. Перед переліком ставлять двокрапку. Перед кожною позицією переліку слід ставити малу літеру української абетки з дужкою, або, не нумеруючи, дефіс (перший рівень деталізації). *Наприклад:*

При проведенні аналізу ризиків підприємства було виділено такі основні загрози:

– обхід мережевого екрану;
– DDoS атака на мережу підприємства;
– зовнішній моніторинг;
– несанкціонований доступ до інформаційних ресурсів;
– викрадення паролів.

Для подальшої деталізації використовують арабські цифри з дужкою. *Наприклад:*

Для забезпечення функціонування мережі виконати таке.

1) заборонити широкомовні адреси;
2) заборонити використання всіх портів для обміну TCP/UDP;
3) обмежити смугу пропускання;
4) проводити аудит вхідного та вихідного трафіку.

Оформлення формул. Між формулою і текстом пропускають один рядок. Кожну формулу записують з нового рядка, симетрично до тексту, курсивом. Умовні літерні позначення в формулі наводять в тексті або зразу ж під формулою Пояснення позначень і символів, які містяться у формулі, якщо це не зроблено раніше, подають безпосередньо під формулою у тій послідовності, в якій вони наведені у формулі або рівнянні. При цьому після формули ставлять кому, а пояснення починають через один рядок із слова «де» без абзацного відступу і без двокрапки. В кінці рядка ставлять крапку

з комою, а після останнього пояснення – крапку. Кожне наступне позначення або символ подають з нового рядка з абзацу. При цьому дозволяється групувати однотипні познаки. Якщо символ позначає фізичну величину, наприкінці пояснення подають відповідну одиницю вимірювання.

Всі формули нумерують в межах розділу арабськими числами. Номер вказують в круглих дужках з правої сторони, в кінці рядка, на рівні закінчення формули. Номер формули складається з номера розділу і порядкового номера формули в розділі, розділених крапкою. Дозволяється виконувати нумерацію в межах всього документа. *Наприклад:*

Потреба в обслуговуванні обчислюється за формулою:

$$D_i = U_i \times \tau / C_0, \tag{3.6}$$

де U_i – з коефіцієнт використання черги i;

C_0 – кількість запитів, виконаних за час τ.

2.2 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 частину, 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 курсової роботи, обов’язковими додатками є:

- Додаток А Технічне завдання;
- Креслення, обумовлені в завданні;
- лістинг коду програми.

2.3 Вміст вступної частини пояснювальної записки

2.3.1Титульний аркуш

Титульний аркуш є першою сторінкою КР, яка не нумерується, але але враховується в загальну кількість сторінок. Згідно з діючим стандартом

титульний аркуш виконується за встановленим зразком. Зразок титульного аркушу пропонується у додатку А.

На титульному аркуші зазначається:

- повна назва організації (Вінницький національний технічний університет);
- структурні підрозділи, в яких виконано КР (факультет і кафедра);
- вид роботи (курсова робота);
- навчальна дисципліна, за якою виконується КР;
- тема КР/КП;
- ім’я та прізвище автора КР/КП із зазначенням шифру академічної групи, коду та найменування спеціальності, за якою навчається здобувач вищої освіти;
- ім’я та прізвище керівника КР із зазначенням посади, наукового ступеня і вченого звання;
- оцінка за 100-бальною шкалою;
- оцінка за шкалою ЄКТС;
- прізвища та ініціали членів комісії по захисту КР;
- місце (місто Вінниця) та рік виконання КР.

На титульному аркуші для курсових робіт подаються: тема курсової роботи; запис «Пояснювальна записка ...» із зазначенням спеціальності, перераховується науковий ступінь та звання керівника.

2.3.2 Індивідуальне завдання

Конкретний зміст кожної курсової роботи та етапи виконання визначає керівник на підставі індивідуального завдання, затвердженого завідувачем кафедри не пізніше ніж за два тижні після початку семестру. Керівник видає індивідуальне завдання до курсової роботи. Індивідуальне завдання в перелік змісту не вноситься та має бути другою сторінкою після титульного аркуша. Зразок індивідуального завдання до курсової роботи наведено в Додатку Б. Керівник роботи пропонує зміст пояснювальної записки, в навчальних цілях зміст може висвітлюватись в індивідуальному завданні.

В залежності від специфіки дисципліни керівник курсової роботи може пропонувати тему, яка вимагає конкретного обґрунтування та розробки індивідуального завдання. Індивідуальне завдання до курсової роботи повинно містити термін видачі, підписи керівника та студента. Індивідуальне завдання на курсову роботу повинно бути підготовлено студентом не пізніше другого тижня з початку навчального семестру, підписано викладачем, що видав завдання, і студентом, що прийняв його до виконання.

2.3.3 Анотація

Анотація призначена для ознайомлення з текстовим документом курсової роботи. Анотація повинна коротко характеризувати мету роботи, засоби, використані 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. Анотація оформлюється на окремому аркуші, який нумерується і враховується у загальній кількості сторінок. Анотація повинна містити прізвище та ініціали автора КР, тему КР, стислий опис змісту та основних результатів КР, а також перелік ключових слів. Обсяг анотації – не більше однієї сторінки. Приклад анотації наведений у Додатку В.

2.3.4 Зміст

Зміст розташовують на третій сторінці безпосередньо після анотації. До змісту включають: вступ; послідовно перелічені назви всіх розділів, підрозділів суті роботи; висновки; список використаних джерел; назви додатків і номери сторінок.. Нумерація у змісті починається із ВСТУПУ (відповідно до нумерації у пояснювальній записці). 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.

Приклад оформлення змісту можна бачити у Додатку Г.

2.4 Вміст основної частини

2.4.1 Вступ

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 курсової роботи. У вступі, і далі за текстом, не дозволяється використовувати скорочені слова, терміни, крім загальноприйнятих.

Вступ висвітлює:

- актуальність та значення теми КР;

- оцінку сучасного стану об’єкта досліджень або розробки, сучасний рівень науки і технології за темою КР;

- світові або регіональні тенденції розв’язання задач, поданих в індивідуальному завданні;

- об’єкт і предмет дослідження;

- мету та завдання КР;

- галузь використання та призначення результатів дослідження;

- взаємозв’язок з іншими роботами, навчальними чи науковими проєктами (за наявності).

Кількість сторінок вступу не повинна перевищувати 2 сторінки.

2.4.2 Передпроєктний аналіз

Проводиться загальний передпроєктний аналіз системи захисту (СЗ) із доведенням актуальності розробки та формулюванням вимог до неї. Даний розділ має бути змістовним, конкретним, зрозумілим, оскільки саме він демонструє знання та навички у галузі аналізу зовнішнього та внутрішнього оточення об’єкта захисту, а також вміння сформулювати вимоги до розроблюваної системи захисту, на основі чого формується технічне завдання – основа для розробки. Рекомендований обсяг підрозділу 8-10 сторінок пояснювальної записки.

2.4.2.1 Системний аналіз предметної області

З точки зору проєктування СЗ в рамках системного аналізу, потрібно здійснити перший етап, тобто провести докладний словесний опис об'єктів предметної області і реальних зв'язків, які присутні між описаними об'єктами. Бажано, щоб даний опис дозволяв коректно визначити всі взаємозв'язки між об'єктами предметної області. У загальному випадку існують два підходи до вибору складу і структури предметної області:

Функціональний підхід – реалізує принцип руху «від завдань» і застосовується тоді, коли заздалегідь відомі функції певної групи осіб і комплексів задач, для обслуговування інформаційних потреб яких створюється розглянута СЗ. У цьому випадку ми можемо чітко виділити мінімальний необхідний набір об'єктів предметної області, які повинні бути описані.

Предметний підхід – коли потреби майбутніх користувачів СЗ жорстко не фіксуються. Вони можуть бути багатоаспектні і вельми динамічні. Не можна точно виділити мінімальний набір об'єктів предметної області, які необхідно описувати. В опис предметної області в цьому випадку включаються такі об'єкти і взаємозв'язки, які найбільш характерні і найбільш істотні для неї. При цьому СЗ, що проєктується, називається предметною, тобто вона може бути використана при вирішенні безлічі різноманітних, заздалегідь не визначених завдань. Конструювання предметної БД в деякому сенсі здається набагато більш привабливим, однак труднощі загального охоплення предметної області з неможливістю конкретизації потреб користувачів може привести до надмірно складної схеми СЗ, яка для конкретних завдань буде неефективною.

Найчастіше на практиці рекомендується використовувати певний компромісний варіант, який, з одного боку, орієнтований на конкретні завдання або функціональні потреби користувачів, а з іншого боку, враховує можливість нарощування нових додатків. Системний аналіз повинен закінчуватися докладним описом інформації про об'єкти предметної області, яка потрібна для вирішення конкретних завдань, формулюванням конкретних завдань, які будуть вирішуватися з використанням даної СЗ з коротким описом алгоритмів їх вирішення, описом вихідних документів, які повинні генеруватися в системі, описом вхідних документів, які служать підставою для обробки даних СЗ. Таким чином потрібно розглянути та проаналізувати об’єкти предметної області: параметри, структуру, функції та задачі, зовнішнє та внутрішнє середовище об’єктів предметної області; інформаційне середовище (ресурси); загрози інформаційної безпеки; потенційні легальні користувачі, потенційні зловмисники (модель порушника інформаційної безпеки), канали витоку інформації з об’єкта захисту (якщо таке передбачається предметною областю). Дати загальну характеристику класу розв’язуваних задач системи захисту по відношенню до кожного із учасників предметної області (для легальних і для зловмисників чи порушників). Зазначити у чому полягає його сутність, чому даному класові задач варто приділяти хоч якусь увагу і присвячувати йому цілий проєкт. Аргументацію варто приводити коротко, виділяючи домінанти. Далі виконується декомпозиція комплексу задач і дається коротка характеристика кожної з задач. При цьому, розглядаються особливості, пов'язані з даним класом задач.

2.4.2.2 Формулювання вимог

Виконайте порівняльний аналіз відомих аналогів (програм, методів, моделей, методик, підходів) проєктованої системи захисту. Виділіть переваги та недоліки.

Здійсніть обґрунтування проєктних рішень по інформаційному, технологічному і програмному забезпеченню комплексу задач.

Проєктні рішення по *інформаційному забезпеченню* будуються з погляду позамашинного і внутрішньомашинного забезпечення і включають наступні питання:

– основні принципи проєктування інформаційного забезпечення комплексу задач;

– обґрунтування складу і змісту результатних масивів і вихідних документів;

– обґрунтування складу, форм представлення вихідної інформації в первинних документах і на машинних носіях;

– обґрунтування вимог до систем класифікації і кодування інформації.

У даному розділі також приділіть увагу обґрунтуванню методів організації інформаційної бази. Розгляньте наступні питання:

– обґрунтування вибору форми збереження даних (база даних або сукупність локальних файлів);

– обґрунтування вибору моделі логічної структури бази даних (ієрархічної, мережевої, реляційної);

– обґрунтування методів організації інформаційних масивів (прообразів файлів), ключів упорядкування тощо.

Виконайте обґрунтування проєктних рішень (вимог) *за технологією збору, передачі, обробки і видачі інформації*, що включає характеристику існуючої технології і підготовку пропозицій по її удосконалюванню, або нової технології, відображаючи:

– вибір способу збору вихідної інформації на основі аналізу доцільності використання технічних засобів збору (реєстраторів, датчиків, лічильників тощо);

– обґрунтування методів передачі інформації в систему (кур'єром, у формі документів, по каналах модемного зв'язку, по каналах локальних обчислювальних мереж, з використанням виділених каналів, дискретним способом через флеш-носії, оптичні носії тощо, в інтерактивному режимі);

– обґрунтування методів забезпечення вірогідності інформації (верифікація, рахунковий контроль тощо);

– обґрунтування технології видачі інформації користувачеві (централізована, децентралізована, розподілена тощо), (на принтер, на екран монітора, у файл).

Обґрунтування проєктних рішень *по програмному забезпеченню* комплексу задач полягає у формуванні вимог до системного, спеціального і прикладного програмного забезпечення. Якщо є необхідність, то можна сформулювати вимоги і по математичному, методичному, метрологічному, лінгвістичному, ергономічному забезпеченні.

На основі проведеного аналізу сформулюйте вимоги до проєктованої системи та відобразіть у технічному завданні (ТЗ). Вимоги групуються у ТЗ по таким розділам та категоріям:

«ВИМОГИ ДО СИСТЕМИ» складається з наступних підрозділів:

1) вимоги до системи в цілому;

2) вимоги до функцій (задач), що виконується системою;

3) вимоги до видів забезпечення.

Склад вимог до системи, що включаються в даний розділ ТЗ на СЗ, установлюють залежно від виду, призначення, специфічних особливостей і умов функціонування конкретної системи.

«ВИМОГИ ДО СИСТЕМИ В ЦІЛОМУ» включають:

– вимоги до структури й функціонування системи;

– вимоги до чисельності й кваліфікації персоналу системи й режиму його роботи;

– показники призначення;

– вимоги до надійності;

– вимоги безпеки;
– вимоги до ергономіки й технічної естетики;
– вимоги до транспортабельності для рухливих АС;
– вимоги до експлуатації, технічного обслуговування, ремонту й збереженню компонентів системи;
– вимоги до захисту інформації від несанкціонованого доступу;
– вимоги по схороненню інформації при аваріях;
– вимоги до захисту від впливу зовнішніх впливів;
– вимоги до патентної чистоти;
– вимоги по стандартизації й уніфікації;
– додаткові вимоги.

«ВИМОГИ ДО ФУНКЦІЙ (ЗАДАЧ), ЩО ВИКОНУЮТЬСЯ СИСТЕМОЮ» включають:

1) по кожній підсистемі перелік функцій, завдань або їхніх комплексів (у тому числі частин, що забезпечують взаємодію, системи), що підлягають автоматизації; при створенні системи у дві або більше черги – перелік функціональних підсистем, окремих функцій або завдань, що вводяться в дію в 1-й і наступних чергах;

2) часовий регламент реалізації кожної функції, завдання (або комплексу завдань);

3) вимоги до якості реалізації кожної функції (завдання або комплексу завдань), до форми подання вихідної інформації, характеристики необхідної точності й часу виконання, вимоги одночасності виконання групи функцій, вірогідності видачі результатів;

4) перелік і критерії відмов для кожної функції, по якій задаються вимоги по надійності.

«ВИМОГИ ДО ВИДІВ ЗАБЕЗПЕЧЕННЯ». Тут залежно від виду системи приводять вимоги до математичного, інформаційного, лінгвістичного, програмного, технічного, метрологічного, організаційного, методичного й інших видів забезпечення системи.

Розробіть склад і зміст робіт із створення СЗ. Він повинен містити перелік стадій і етапів робіт із створення системи, строки їхнього виконання, перелік виконавців робіт. Побудуйте мережевий графік та діаграму Ганта проєкту. Розробіть технічне завдання на СЗ згідно ГОСТ 34.602-89 або НД ТЗІ 3.7-001-99 (у разі розробки комплексної СЗІ). Також за бажанням студента ТЗ може бути представлено у вигляді документа «Software Requirements Specification» згідно стандарту ISO/IEC/IEEE 29148:2018.

2.4.3 Технороботче проєктування

Проєкт СЗ розробляється на підставі та у відповідності до ТЗ. Під час розробки проєкту СЗ обґрунтовуються і приймаються проєктні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію

різних компонентів СЗ, а також різних заходів і способів захисту інформації. Проєкт СЗ виконується на таких стадіях: ескізний проєкт, технічний проєкт, робочий проєкт. Дозволяється вилучати етап «Ескізний проєкт», а також поєднувати етапи «Технічний проєкт» і «Робочий проєкт» в один етап «Техноробочий проєкт». Для всіх стадій розробки проєкту СЗ склад документації визначається ТЗ на СЗ, види та зміст – ГОСТ 34.201, НД ТЗІ 2.5-004. Документація на програмні засоби виконується згідно з комплексом стандартів ЄСПД, а на технічні засоби – згідно з комплексом стандартів ЄСКД**.** Рекомендований обсяг підрозділу – 10-20 сторінок пояснювальної записки.

2.4.3.1 Технічне проєктування

Розробку технічного проєкту можна поділити на 4 етапи (ГОСТ 34.601–90 «Автоматизовані системи. Стадії створення», НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»):

1. Розробка проєктних рішень по системі захисту та її частинах.
2. Розробка документації на систему захисту та її частини.
3. Розробка документації на постачання засобів захисту інформації та/або технічних вимог (технічних завдань) на їх розробку.
4. Розробка завдань на проєктування в суміжних частинах проєкту.

Перелік документів, що створюються на стадії «Технічний проєкт», визначається документом ГОСТ 34.201-89. Вимоги до змісту документів технічного проєкту наведені в керівному документі по стандартизації РД 50-34.698-90.

На першому етапі виконується розробка: загальних проєктних рішень, необхідних для реалізації вимог ТЗ на СЗ; рішень щодо структури СЗ (організаційної структури, структури технічних і програмних засобів), математичних моделей та алгоритмів функціонування, умов використання засобів захисту; рішень щодо архітектури СЗ та механізмів реалізації, визначених функціональним профілем послуг безпеки інформації; плану організаційних заходів щодо підготовки об’єкта до введення системи в дію. Здійснюються організаційно-технічні заходи щодо забезпечення послідовності розробки СЗ, архітектури, середовища розробки, випробувань, середовища функціонування та експлуатаційної документації СЗ у відповідності до заданих рівнем гарантій реалізації послуг безпеки згідно із специфікаціями НД ТЗІ 2.5-004, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010.

На другому етапі здійснюють розробку, оформлення, погодження та затвердження документації в обсязі, необхідному для опису повної сукупності прийнятих проєктних рішень і достатньому для наступного виконання робіт, завдань на проєктування будівель, помешкань, у тому числі суміжних частин проєкту будівництва об’єкта.

На третьому етапі здійснюють оформлення документації на постачання засобів захисту або продукції, що містить їх у своєму складі, для

комплектації СЗ. Якщо необхідної продукції немає на ринку засобів захисту, то визначаються технічні вимоги (складаються технічні завдання) на розроблення відповідних засобів.

На четвертому етапі здійснюють розробку, оформлення, погодження і затвердження завдань на проєктування в суміжних частинах проєкту для виконання будівельних, електротехнічних, санітарно-технічних та інших підготовчих робіт, які пов’язані із створенням системи.

Під час розробки положень про забезпечуючі системи враховуються дані, зібрані у процесі обстеження об'єкта дослідження. Розглянемо положення кожної забезпечуючої підсистеми.

Організаційне забезпечення це сукупність документів, які встановлюють організаційну структуру, права і обов`язки користувачів і експлуатаційного персоналу в умовах функціонування, перевірки та забезпечення працездатності ІС.

Методичне забезпечення це сукупність документів, що описують технологію функціонування СЗ, методи вибору і використання користувачами технологічних прийомів для отримання конкретних результатів при функціонуванні ІС.

Інформаційне забезпечення це сукупність форм документів, нормативної бази та реалізованих рішень щодо обсягів, розміщення і форм існування інформації, яка використовується в інформаційній системі при її функціонуванні і поділяється на позамашинне і внутрішньомашинне інформаційне забезпечення. Усю інформацію, що обробляється в СЗ, можна поділити на вхідну, проміжну та вихідну. Після розробки позамашинного та внутрішньомашинного інформаційного забезпечення проєктується технологічний процес обробки даних в ІС.

Технічне забезпечення це сукупність всіх технічних засобів, що використовуються при функціонуванні СЗ. КТЗ — сукупність взаємопов'язаних єдиним управлінням автономних технічних засобів збирання, накопичення, обробки, передачі, ведення та подання інформації, пристроїв управління ними. Сюди ж належать засоби оргтехніки, призначені для організації тривалого збереження (накопичення) інформації і здійснення інформаційного обміну між різними технічними засобами.

Математичне забезпечення це сукупність математичних методів, моделей і алгоритмів, що використовуються в ІС.

Програмне забезпечення це сукупність програм на носіях даних і програмних документів, призначених для налагодження, функціонування та перевірки працездатності СЗ.

Лінгвістичне забезпечення це сукупність засобів і правил для формалізації природної мови, що використовуються при спілкуванні користувачів і експлуатаційного персоналу із СЗ.

Правове забезпечення це сукупність правових норм, які регламентують правові відношення при функціонуванні СЗ та юридичний статус

результатів її функціонування.

Ергономічне забезпечення це сукупність реалізованих рішень в СЗ по погодженню психологічних, психофізіологічних, антропометричних, фізіологічних характеристик і можливостей користувачів з технічними характеристиками СЗ і параметрами робочого середовища на робочих місцях персоналу СЗ.

У курсовій роботі розробку рішень по технічному проєкту системи захисту виконайте та подайте інформацію у ПЗ з орієнтацією на наступні підрозділи:

– *Функціональна й організаційна структура системи*:

1) обґрунтування виділення підсистем системи захисту, їх перелік та призначення;
2) перелік завдань, що вирішуються в кожній підсистемі, з короткою характеристикою їх змісту;
3) схема інформаційних зв'язків між підсистемами і між завданнями в рамках кожної підсистеми.

– *Постановка завдань і алгоритми вирішення*:

1) організаційно-економічна сутність задачі (найменування, мета рішення, короткий зміст, метод, періодичність і час виконання завдання, способи збору і передачі даних, зв'язок задачі з іншими задачами, характер використання результатів рішення, в яких вони використовуються);
2) математична модель задачі (структурна і розгорнута форма подання);
3) вхідна оперативна інформація (характеристика показників, діапазон зміни, форми подання);
4) нормативно-довідкова інформація (НДІ) (зміст і форми подання);
5) інформація, що зберігається для зв'язку з іншими завданнями;
6) інформація, що накопичується для наступних варіантів розв'язання задачі;
7) інформація щодо внесення змін (система внесення змін і перелік інформації, яка піддається змінам);
8) алгоритм вирішення задачі (послідовність етапів розрахунку, схема, розрахункові формули);
9) контрольний приклад (набір заповнених даними форм вхідних документів, умовні документи з накопичуваної і збереженої інформацією, форми вихідних документів, заповнені за результатами рішення економіко-технічної задачі і відповідно до розробленого алгоритму розрахунку).

– *Організація інформаційної бази*:

1) джерела надходження інформації та способи її передачі;
2) сукупність показників, що використовуються в системі;
3) склад документів, терміни і періодичність їх надходження;
4) основні проєктні рішення по організації фонду НДІ;
5) склад НДІ, включаючи перелік реквізитів, їх визначення, діапазон зміни і перелік документів НДІ;

6) перелік масивів НДІ, їх обсяг, порядок і частота коригування інформації;
7) структура фонду НДІ з описом зв'язку між його елементами; вимоги до технології створення і ведення фонду;
8) методи зберігання, пошуку, внесення змін і контролю;
9) визначення обсягів і потоків інформації НДІ;
10) контрольний приклад по внесенню змін до НДІ;
11) пропозиції щодо уніфікації документації.

– *Система математичного забезпечення*:

1) обґрунтування структури математичного забезпечення;
2) обґрунтування вибору системи програмування;
3) перелік стандартних програм.

– *Принцип побудови комплексу технічних засобів:*

1) опис і обґрунтування схеми технологічного процесу обробки даних;
2) обґрунтування і вибір структури комплексу технічних засобів і його функціональних груп;
3) обґрунтування вимог до розробки нестандартного обладнання;
4) комплекс заходів щодо забезпечення надійності функціонування технічних засобів.

– *Заходи з підготовки об'єкта до впровадження системи*:

1) перелік організаційних заходів щодо вдосконалення бізнес-процесів;
2) перелік робіт з впровадження системи, які потрібно виконати на стадії робочого проєктування, із зазначенням термінів і відповідальних осіб.

2.4.3.2 Робоче проєктування системи захисту

На етапі «Робочий проєкт» (НД ТЗІ 3.7-003-2005) або «Робоча документація» (ГОСТ 34.601–90) ведуться роботи щодо практичної реалізації положень, закладених в проєкті. Робоча документація розробляється на основі затверджених технічного завдання і технічного проєкту і затвердженню не підлягає. Мета робочого проєктування – складання технічної документації для налагодження і впровадження системи захисту, для проведення приймально-здавальних досліджень, а також для забезпечення нормального забезпечення функціонування СЗ.

Основні роботи на етапі робочого проєктування:

1. Розробка робочої документації на систему та її частини.

2. Розробка чи адаптація системи.

На першому етапі здійснюється розробка робочої документації, яка містить всі необхідні й достатні відомості для забезпечення виконання робіт з введення інформаційної системи в дію та її експлуатації, а також для підтримання рівня експлуатаційних характеристик (якості) системи згідно з прийнятими проєктними рішеннями, її оформлення, погодження і затвердження. Це технологічні інструкції з обробки даних, інструкції для роботи в умовах функціонування розробленої системи, порадник користувача.

Можна виділити такі роботи:

1) прийняття рішень щодо організації розробки робочої документації;

2) розробка загальносистемних проєктних рішень;

3) розробка проєктної документації з видів забезпечення;

4) оформлення, погодження, затвердження в установленому порядку.

Роботи з інформаційного забезпечення:

1) розробка експлуатаційної документації з інформаційного забезпечення, до якої входить розробка уніфікованих форм документів і підготовка класифікаторів;

2) перевірка інформаційно-логічної структури бази даних;

3) розробка інструкції для створення і ведення бази даних.

Роботи з організаційного забезпечення:

1) уточнення функцій і конкретизація складу робіт персоналу інформаційної системи, розробка положень та інструкцій усіх видів, формуляру системи;

2) розробка технологічного процесу обробки даних, який складається з технологічного процесу отримання і обробки даних. Розробка керівництва користувача.

На другому етапі здійснюється адаптація чи розробка програмних модулів системи захисту, інформаційних виробів, програмної і експлуатаційної документації.

У ході розробки робочої документації замовник:

1) забезпечує приймання до дослідної експлуатації;

2) завершує під методичним керівництвом розробника формування інформаційної бази і організовує її експлуатацію;

3) передає на вимогу розробника дані, необхідні для перевірки задач на контрольних приладах;

4) організовує приймання програм, надаючи розробникові магнітні носії та машинний час;

5) виконує основні організаційно-технічні заходи з підготовки підприємства до введення системи в дію.

Розробник розробляє та оформлює технічну документацію з усіх видів забезпечення і перевіряє програми. Склад і структура проєктної документації на стадіях «Технічний проєкт» і «Робоча документація» визначаються ГОСТ 34.201–89 «Види, комплектність та позначення документів при створенні автоматизованих систем», РД 50-34.698-90 «Автоматизовані системи. Вимоги до змісту документів». Робочу документацію також можна поділити на дві частини: програмні документи (технічне завдання, специфікація, текст програми, опис програми, програма та методика випробувань, специфікація тощо) та експлуатаційній документи (формуляр, опис застосування, керівництво користувача, керівництво програміста, відомість експлуатаційних документів тощо). У ПЗ до КР презентуйте та прокоментуйте основні програмні коди проєктованої системи захисту. Розробіть документ «Текст програми» згідно ГОСТ 19.401-78 та презентуйте його у додатках до ПЗ. Наведіть основні принципові аспекти щодо використання проєктованої

системи із використанням відповідних екранних форм та коментарів до них. Розробіть документ «Керівництво оператора» згідно ГОСТ 19.505-79 або «Керівництво користувача» згідно РД 50-34.698-90 та подайте його у додатках до ПЗ.

2.4.4 Впровадження системи захисту

На етапі введення СЗ в дію виконуються такі роботи:
- підготовка СЗ до введення в дію;
- навчання користувачів;
- комплектування СЗ;
- будівельно-монтажні роботи;
- пусконалагоджувальні роботи;
- попередні випробування;
- дослідна експлуатація;
- приймальні випробовування (державна експертиза).

Одним із основних видів робіт на даному етапі є випробовування системи а саме її тестування та перевірка відповідності до вимог ТЗ. Тому даний розділ ПЗ саме присвячений тестуванню проектованої СЗ та оцінки її ефективності. Рекомендований обсяг підрозділу – 10-15 сторінок пояснювальної записки.

2.4.4.1 Проведення випробувань системи захисту

Метою випробувань є перевірка працездатності СЗ та визначення можливості прийняття її у дослідну експлуатацію. Під час випробувань перевіряються працездатність СЗ та відповідність її вимогам ТЗ. Випробування проводяться згідно з програмою та методиками випробувань відповідно до ДСТУ 2853-94. Програму й методику випробувань готує розробник СЗ, а узгоджує замовник. Програма та методики випробувань, протоколи випробувань розробляються та оформлюються згідно з вимогами ГОСТ 19.301-79 або РД 50-34.698.

Виконайте тестування розробленої системи захисту скориставшись різними методиками та підходами («біла скринька», «чорна скринька» тощо). Розробіть та виконайте необхідні тести. Самі методики тестування та результати їх застосування відобразіть у ПЗ. Після кожного тесту зробіть висновок. За результатами тестування за бажанням можна сформувати документ «Акт тестування» та включити його у додатки до КР. Більш ефективним, згідно принципів тестування, буде залучення незалежного тестувальника, наприклад, колегу по групі. При цьому йому потрібно надати усю необхідну документацію, а саме технічне завдання, схеми алгоритмів, текст програми, керівництво користувача, опис системи, розроблені тести тощо. Незалежний тестувальник може доповнити набір тестів або ж сформувати свій. За результатами тестування він формує свій «Акт тестування». Ви у свою чергу можете виступати незалежним тестувальником для іншого

студента. У разі отримання негативних результатів виконання тестів вкажіть на можливі причини їх отримання та виконайте налагодження системи із повторним тестуванням до отримання бажаного позитивного результату.

Розробіть документ «Програма та методика випробувань» та подайте його у додатку.

2.4.4.2 Оцінка ефективності системи захисту

Оцінку ефективності системи захисту можна виконати за економічними, технічними та соціальними показниками. Розрахуйте показники економічної ефективності розробленої системи захисту та подайте результати у ПЗ. Для розрахунку скористайтесь найбільш прийнятою методикою для проєктованої системи. Можете при необхідності скористатись декількома методиками та порівняти отримані результати. Основними економічними показниками є капітальні та експлуатаційні витрати на розробку та впровадження системи, економічний ефект від розробки та впровадження, термін окупності системи тощо. Розрахуйте показники технічної ефективності розробленої системи захисту та подайте результати у ПЗ. У якості таких показників може бути підвищення швидкодії (швидкості) або точності (достовірності) обробки (спрацювання, обчислень, передавання, шифрування, кодування, діагностування, розпізнавання, відображення, аналізу тощо) інформації. Також показники технічної ефективності можуть бути відображені у зменшенні часу обробки, зменшенні суб'єктивності при прийнятті рішень, підвищенні захищеності системи тощо. Відобразіть соціальний ефект від розробки системи захисту, якщо таке передбачалося у ТЗ. Можете запропонувати із відповідним обґрунтуванням власні показники оцінки ефективності системи захисту інформації. Проведіть порівняльний аналіз функціоналу та вартісних показників вашої системи з аналогічними.

2.5 Висновки

Висновки оформляють з нової пронумерованої сторінки посередині великими літерами більш високої насиченості. У висновках приводяться основні результати роботи над курсовим проєктом. На основі результатів роботи надаються обґрунтовані висновки щодо переваг та недоліків застосування запропонованого рішення. Наводяться недоліки та переваги розробленої системи, труднощі при розробці та причини, що їх обумовили і можливі шляхи їх подолання, можливі рекомендації прикладного застосування та шляхи (перспективи) удосконалення розробленої системи захисту.

2.6 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 8302:2015 «Інформація та документація. Бібліографічне посилання», 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.

2.7 Додатки

Обов'язковим додатком є технічне завдання. Технічне завдання розробляється студентом самостійно на основі індивідуального завдання та проведеного передпроєктного аналізу (1-й розділ КР). Зразок технічного завдання наведено у Додатку Д. Також обов'язковими додатками є текст програми (Додаток Е), керівництво користувача (Додаток Ж), програма і методика випробувань (Додаток И). Інші додатки повинні містити матеріал, який не увійшов в основні розділи пояснювальної записки: лістинг програм, підпрограм та функцій, результати тестування програми у вигляді образів екранів, таблиць, графіків, 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 тощо, що пояснюють наведений текст. Кожен додаток потрібно починати з нової сторінки, вказуючи зверху посередині рядка слово «ДОДАТОК» і через пропуск – його позначення. Додатки позначають послідовно великими українськими буквами, за винятком букв *Ґ, Є, З, І, Ї, Й, О, Ч, Ь*, наприклад, ДОДАТОК А, ДОДАТОК Б тощо. Якщо додатків більше ніж букв, то продовжують позначати арабськими цифрами. Дозволяється позначати додатки латинськими буквами, за винятком букв *I* і *O*.

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.

3 РОЗРОБКА І ОФОРМЛЕННЯ ІЛЮСТРАТИВНОЇ ЧАСТИНИ

Підсумком виконання курсової роботи є розробка ілюстративної частини, яка демонструє основні результати виконаної розробки.

Ілюстративна частина КР є набором демонстраційного матеріалу у

вигляді рисунків, світлин, 3D моделей, графіків, схем тощо, які розкривають сутність основної частини. Ілюстративна частина не потребує обов'язкового дотримання вимог стандартів і може бути оформлена як один додаток. Вимоги до ілюстративної частини зазначаються в індивідуальному завданні.

4 ГРАФІК ВИКОНАННЯ КУРСОВОЇ РОБОТИ І ПОРЯДОК ЙОГО ЗАХИСТУ

Рекомендується такий графік виконання курсової роботи (табл. 4.1), який враховує самостійну роботу студентів під час 2-го (згідно навчального плану) семестру (18 тижнів). Упродовж теоретичного семестру керівник проводить періодичні консультації з питань виконання КР та контролює дотримання графіка виконання КР здобувачами вищої освіти. Здобувачі вищої освіти мають самостійно виконувати індивідуальне завдання, дотримуючись встановленого графіка.

КР виконується у вигляді комп'ютерного файлу за допомогою будь-якого програмного текстового редактора, який здатний забезпечити виконання вимог до оформлення КР. Здобувачі вищої освіти можуть надсилати на перевірку завершений етап або повний текст КР через інструмент «Файл-Експрес» системи JetIQ у вигляді одного файлу у форматі Portable Document Format (*.pdf). Керівник зобов'язаний дати відповідь на надісланий файл протягом семи діб з моменту отримання файлу. У відповіді керівник має вказати, що він приймає етап чи повний текст КР до захисту або зазначити, що потрібно виправити/доопрацювати. Під час прийняття рішення враховується якість виконання завдань та оформлення КР, а також відповідність вимогам академічної доброчесності. Перевірці на плагіат підлягає або повний текст КР, або та частина КР, яка передбачає написання унікального тексту. Рішення про обсяг і предмет перевірки для КР приймається на засіданні кафедри. У разі виявлення ознак академічного плагіату, інших ознак академічної недоброчесності або якщо рівень унікальності тексту для визначених складає менше 60%, така КР не допускається до захисту.

Повернення КР для виправлення/доопрацювання допускається тільки протягом теоретичного семестру. Файли, надіслані після завершення теоретичного семестру, вважаються остаточними, а їх заміна або виправлення не допускаються. Якщо КР виконано у повному обсязі, у відповідності до індивідуального завдання, не містить ознак академічної недоброчесності, не містить суттєвих помилок, оформлена згідно з встановленими вимогами та надіслана здобувачем вищої освіти у вигляді одного файлу у форматі Portable Document Format (*.pdf), керівник приймає КР до захисту, про що повідомляє здобувача вищої освіти у відповіді на файл, надісланий через інструмент «Файл-Експрес» системи JetIQ. Якщо остаточний файл КР виконано не в повному обсязі, або не у відповідності до індивідуального завдання, або він містить ознаки академічної недоброчесності, або суттєві

помилки, або не оформлено згідно з встановленими вимогами, або файл не надійшов через інструмент «Файл-Експрес» системи JetIQ (станом на визначений у розкладі день захисту), така КР визнається керівником недопущеною до захисту із виставленням незадовільної оцінки у відомість успішності (від 0 до 59 балів). Якщо оцінка за стобальною шкалою склала від 35 до 59 балів включно, то здобувач вищої освіти має право на доопрацювання і захист КР з виставленням оцінки у другу відомість. Якщо оцінка за стобальною шкалою склала від 0 до 34 балів включно, то здобувач вищої освіти вважається таким, що має академічну заборгованість. Для її ліквідації здобувач має виконати КР за новою темою (або зміненим індивідуальним завданням) у відповідності до «Положення про порядок ліквідації академічної заборгованості, академічної різниці та надання платної послуги з проведення занять з вивчення окремої навчальної дисципліни понад обсяги, встановлені навчальним планом».

Таблиця 4.1 – Графік виконання курсової роботи

Зміст розділу	Термін виконання
Отримання завдання на курсову роботу, збір матеріалу, аналіз літературних джерел, пошук аналогів	1-2 тижд.
Системний аналіз предметної області	3-4 тижд.
Формулювання вимог до системи захисту. Розробка технічного завдання	5-6 тижд.
Розробка технічного проєкту системи захисту. Розробка структури системи. Розробка та опис математичних моделей. Побудова алгоритмів. Вибір програмних засобів	7-9 тижд.
Розробка робочого проєкту. Розробка програмних та інтерфейсних модулів системи. Розробка програмного коду системи. Розробка керівництва користувача	10-12 тижд.
Розробка програми та методики випробувань. Випробування системи захисту. Оформлення результатів тестування	13-14 тижд.
Оцінка ефективності системи захисту. Оформлення пояснювальної записки	15-16 тижд.
Здача курсової роботи на попередню перевірку: демонстрація роботи програми та чернетки пояснювальної записки (можливий її електронний варіант)	17 тижд.
Корегування і доповнення (при необхідності) згідно зауважень керівника курсової роботи, врахування і виправлення пояснювальної записки	17 тижд.
Захист курсової роботи	18 тижд.

Перевірку КР на наявність помилок у їх змісті та оформленні, нормоконтроль (за необхідності) здійснює керівник КР, а в разі його тимчасової відсутності – інший науково-педагогічний працівник відповідної кафедри, визначений розпорядженням завідувача кафедри.

Готовність до захисту курсової роботи визначає керівник за результатами попередньої перевірки якості пояснювальної записки. Записка повинна

бути здана керівнику на перевірку не менш, як за тиждень до визначеного терміну захисту проєкту. Якщо робота виконана в повному обсязі і не має принципових помилок, керівник допускає студента до захисту. В іншому випадку робота повертається студенту на доопрацювання. Після позитивного висновку про готовність курсової роботи студент має захистити його перед комісією у складі двох викладачів, які призначені кафедрою.

5 ОЦІНЮВАННЯ КУРСОВОЇ РОБОТИ

Оцінюється курсова робота членами комісії після її захисту студентом у балах і за національною шкалою оцінок. Загальна кількість балів включає (табл. 5.1) оцінки змісту роботи (до 45 балів), оформлення пояснювальної записки (до 25 балів), ілюстративної частини (до 10 балів) та захисту (до 20 балів).

Таблиця 5.1 – Оцінювання курсової роботи

Розробка	Пояснювальна записка	Ілюстрат. частина	Захист	Всього
45	25	10	20	100

При оцінюванні курсової роботи за кредитно-модульною системою враховуються:

- кваліфікаційний рівень (фаховість, дотримання стандартів) підготовки захисту ІКС;
- обґрунтування актуальності теми курсової роботи;
- відповідність назв і змісту структурних елементів пояснювальної записки цілям, завданням та особливостям побудови систем захисту ІКС;
- грамотність викладу змісту пояснювальної записки, відповідність її вимогам щодо оформлення робіт;
- вміння студента представляти результати курсової роботи.

Підготовка курсової роботи – сумарно 100 балів, у тому числі:

Якість розробки – 45 бали:

- фахова вмотивованість рішень – 15 бали;
- логічність і послідовність рішень – 15 балів;
- обґрунтованість та оптимальність обраних рішень – 10 балів;
- дотримання стандартів побудови систем захисту – 5 балів.

Зміст пояснювальної записки – 25 балів:

- відповідність структурних розділів визначеній тематиці та вимогам до даного типу робіт: *вступ, основна частина, висновки, додатки* – 15 балів.
- відповідність оформлення ПЗ стандартам –5 балів;
- наявність посилань та списку використаних джерел – 3 бали;
- дотримання граматичних і стилістичних правил – 2 бали.

Зміст ілюстративної частини – 10 балів:

- відповідність ілюстративної частини завданню – 5 балів;
- відповідність ілюстративної частини тексту пояснювальної записки –3

бали;

- відповідність ілюстративної частини стандартам –2 бали.

Захист курсової роботи – 20 балів:

- вміння студента логічно структурувати доповідь та доводити до присутніх у стислій формі основні результати – 10 балів;

- відповіді на запитання (чіткість формулювання та відповідність запитанню) – 10 балів.

Для переведення суми балів в оцінку ECTS використовуємо шкалу оцінювання, що наведена в таблиці 5.2.

Таблиця 5.2 – Шкала оцінювання

Сума балів за всі види навчальної діяльності	Оцінка ECTS
90-100	**A**
82-89	**B**
75-81	**C**
64-74	**D**
60-63	**E**
35-59	**FX**
0-34	**F**

100 балів – робота бездоганна за виконанням, супроводжується змістовною, належно оформленою пояснювальною запискою і бездоганно захищена (доповідь, відповіді на питання тощо), а також в роботі наявні елементи наукової новизни та практичної цінності за напрямом курсової роботи.

6 ВАРІАНТИ ЗАВДАНЬ

Варіанти обираються відповідно до номера у журналі академічної групи або студент пропонує свій із попереднім узгодженням з науковим керівником.

Типові варіанти для виконання КР:

1. Проєктування програмного засобу для обфускації.
2. Проєктування системи захисту від SQL-ін'єкцій.
3. Проєктування програмного засобу для захисту даних в ОС Android.
4. Проєктування програмного засобу для виявлення прихованих процесів в ОС Windows.
5. Проєктування програмного засобу для захисту виконуваних файлів за допомогою цифрового підпису.
6. Проєктування системи виявлення DDOS атак на основі самоорганізаційних карт Кохонена.
7. Проєктування програмного засобу для аналізу ШПЗ в ОС Android.
8. Проєктування засобу для захисту баз даних в ОС Android.
9. Проєктування засобу захисту від DDoS-атак.
10. Проєктування системи захисту файлів на платформі.
11. Проєктування системи захисту від НСД до програмного забезпечення з прив'язкою до мережевих параметрів.
12. Проєктування засобу для оцінювання ризиків інформаційної безпеки на основі методу ієрархії.
13. Проєктування СППР при виборі програмно-технічних засобів захисту від загроз ІБ підприємства.
14. Проєктування системи захисту WEB-ресурсів.
15. Проєктування системи стеганографічного захисту.
16. Проєктування системи захисту від несанкціонованого доступу.
17. Проєктування програмного засобу методом хешування.
18. Проєктування програмного засобу захисту від модифікації файлів.
19. Проєктування засобу захисту комунікації методом шифрування (запропонувати шифр).
20. Проєктування системи захисту мовної інформації в каналах зв'язку.
21. Проєктування програмного захисту методом цифрових водяних знаків.
22. Проєктування системи захисту від аналізу дампа пам'яті в ОС Windows.

23. Проєктування системи виявлення аномалій на основі нейромереж.

24. Проєктування засобу для шифрування файлів на основі еліптичних кривих з використанням прив'язки.

25. Проєктування системи захисту програмного забезпечення з прив'язкою до флеш-носія.

26. Проєктування системи захисту з прив'язкою до апаратного забезпечення комп'ютера.

27. Проєктування системи захисту даних на основі стеганографічних методів.

28. Проєктування системи біометричної автентифікації.

29. Проєктування системи виявлення прихованої інформації методом стеганоаналізу.

30. Проєктування системи захисту з прив'язкою до місцевості.

31. Проєктування засобу для авторизації на основі стеганографії.

32. Проєктування системи для автентифікації за допомогою блокового шифру.

33. Проєктування системи для автентифікації за допомогою симетричного шифру.

34. Проєктування системи виявлення фейкових новин.

35. Проєктування системи виявлення вебатак на основі великих мовних моделей.

36. Проєктування системи захисту від витоку інформації.

37. Проєктування системи тестування на проникнення вебзастоунку.

38. Проєктування системи тестування на проникнення мобільного застосунку.

39. Проєктування системи тестування на проникнення веб-API.

40. Проєктування системи тестування безпеки ШІ-застосунку.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. ДСТУ ISO/IEC 27032:2024. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2023, IDT). [Чинний від 2025-02-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2025.

2. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). [Чинний від 2023-08-22]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2023.

3. ДСТУ ISO/IEC 27002:2023. Інформаційна безпека, кіберзахист та захист конфіденційності. Засоби контролювання інформаційної безпеки. [Чинний від 2023-08-22]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2023.

4. ДСТУ ISO/IEC 27005:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. [Чинний від 2023-08-22]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2023.

5. 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 : затв. наказом ДСТСЗІ СБ України від 20.12.2000 р. № 60. Київ, 2000. 8 с.

6. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі : затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22. Київ, 1999. 35 с.

7. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі : затв. наказом ДСТСЗІ СБ України від 08.11.2005 р. № 125. Київ, 2005. 22 с.

8. Agile-маніфест розробки програмного забезпечення / К. Бек, М. Бідл та ін. ; пер.: О. Солнцев та ін. Ward Cunningham, 2001. URL: https://agilemanifesto.org/iso/uk/manifesto.html (дата звернення: 01.02.2025).

9. Дудатьєв А. В. Комплексна інформаційна безпека соціотехнічних систем: моделі впливу та захисту : монографія. Вінниця : ВНТУ, 2017. 128 с.

10. Катренко А. В. Управління IT-проектами. Львів: Новий світ-2000, 2024. Кн. 1. Стандарти, моделі та методи управління проектами. 550 с.

11. Кібербезпека: web-технології : навчально-довідковий посібник / С. П. Євсеєв, А. М. Ткачов, В. О. Алексієв, Ю. М. Рябуха; ХНЕУ ім. С. Кузнеця. Львів : Новий Світ-2000, 2023. 390 с.

12. Когут Ю. І. Кібервійна та безпека об’єктів критичної інфраструктури. Київ : Сідкон, 2021. 315 с.

13. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання CISCO : навч. посіб. Львів : Вид-во Львівської політехніки, 2021. 232 с.

14. Косинський М. DevOps+Security, SecDevOps, DevSecOps: в чому різниця і що обрати. *DOU*. URL: https://dou.ua/lenta/articles/devops-security (дата звернення: 01.02.2025).

15. Кузьміних В. О., Коваль О. В., Тараненко Р. А. Моделі та засоби управління ІТ-проєктами. Київ : КПІ ім. І. Сікорського, 2023. 222 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/057779d8-d88f-4cef-b2d5-67086a013516/content (дата звернення: 01.02.2025).

16. Куперштейн Л., Дудатьєв А., Войтович О., Ясинська Я. Модель політики інформаційної безпеки для об`єктів критичної інфраструктури. Вимірювальна та обчислювальна техніка в технологічних процесах. 2021. № 2. С. 30-38. URL: https://vottp.khmnu.edu.ua/index.php/vottp/article/view/4/4 (дата звернення: 01.02.2025).

17. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навч. посіб. 2-ге вид., стер. Львів : Новий світ-2000, 2022. 678 с.

18. Остапов, С. Е., Євсеєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту : навч. посіб. Львів : Новий Світ- 2000, 2023. 678 с.

19. Поради (рекомендації) щодо створення КСЗІ в ІКС, які використовуються для надання послуг доступу до мережі Інтернет. *Державна служба спеціального зв'язку та захисту інформації.* URL: https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet (дата звернення: 01.05.2024).

20. Проектування, введення в дію та супроводження КСЗІ : навч. посіб. / В. Д. Козюра, В. О. Хорошко та ін. Ніжин : ФОП Лук'яненко В. В. ТПК «Орхідея», 2019. 240 с.

21. Стандарт з управління проєктами та Настанова до зводу знань з управління проєктами (Настанова PMBOK). 7-е вид. Бібліотека Конгресу США, 2021. 370 с. URL: file:///D:/Documents/Downloads/PMBOK7_Ukr_ForPersonalUseOnly.pdf (дата звернення: 01.02.2025).

22. Швабер К., Сазерленд Д. Посібник зі Скраму™: повний навчальний посібник зі Скраму: правила гри. Листопад, 2020. URL: https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-Ukrainian.pdf (дата звернення: 01.02.2025).

23. Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. Комплексні системи захисту інформації : навч. посіб. Вінниця : ВНТУ, 2018. 118 с. URL: https://web.posibnyky.vntu.edu.ua/fmib/

41yaremchuk_kompleksni_systemy_zahystu_informaciyi/index.html (дата звернення: 01.02.2025).

24. A Guide to the Business Analysis Body of Knowledge (BABOK Guide). Van Haren Pablishing, 2015. P. 512.

25. Automated code quality and security reviews. *Sonar Qube server* . URL: https://www.sonarqube.org (дата звернення: 01.05.2024).

26. Building Secure and Reliable Systems: Best Practices for Designing, Implementing and Maintaining Systems / H. Adkins et al. O'Reilly Media, 2020. P. 400.

27. DDoS-attack detection using artificial neural networks in Matlab / L. M. Kupershtein, T. B. Martyniuk, O. P.Voitovych et al. *Photonics Applicationsin Astronomy, Communications, Industry, and High-Energy Physics Experiments.* 2019. Vol. 11176. URL: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11176/111761S/DDoS-attack-detection-using-artificial-neural-networks-in-Matlab/10.1117/12.2536478.full?webSyncID=ebebcdc8-a3c3-4385-ab16-e9b0e662b676&sessionGUID=328c99b8-8c76-1318-3e4b-47cc4170710e (дата звернення: 01.02.2025).

28. Fernandez E. B., Yoshioka N., Washizaki H., Yoder J. Abstract security patterns and the design of secure systems. *Cybersecurity*. URL: https://doi.org/10.1186/s42400-022-00109-w (дата звернення: 01.02.2025).

29. Hoffman A. Web Application Security: Exploitation and Countermeasures for Modern Web Applicatioins. O'Reilly Media Inc., 2024. P. 446.

30. Kupershtein, L., Martyniuk, T., Voitovych, O., Borusevych, A. Remote Host Operation System Type Detection Based on Machine Learning Approach. *CEUR Workshop Proceedings.* 2021. Pp. 65–81.

31. Souppaya M., Scarfone K., Dodson D. Secure Software Development Framework. *NIST Special Publication 800-218.* URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf (дата звернення: 01.05.2024).

32. Step By Step Guide: How to Write a Security Pattern. *SecurityPatterns.io*. URL: https://securitypatterns.io/docs/how-to-write-a-security-pattern (дата звернення: 01.05.2024).

ДОДАТОК А
Приклад оформлення титульного аркуша

Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп’ютерної інженерії
Кафедра захисту інформації

КУРСОВА РОБОТА
з дисципліни «Проєктування систем кібербезпеки»
на тему: «Проєктування системи захисту від SQL-ін'єкцій»

Студента групи 1БС-24м
Спеціальності F5 Кібербезпека та захист інформації
ОПП «Безпека інформаційних і комунікаційних систем»
_____ Б. С. Іваненко
Керівник: доц. кафедри ЗІ,
канд. техн. науке, доцент
_____ Л. М. Куперштейн

Кількість балів: _____
Оцінка ECTS _____

Члени комісії:

_____

_____

м. Вінниця – 2025 р.

ДОДАТОК Б

Приклад оформлення індивідуального завдання

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти ІІ (магістерський)
Спеціальність – F5 Кібербезпека та захист інформації
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Зав. кафедри ЗІ,
д-р. техн. наук, проф.
_____В. А. Лужецький
(підпис)
«___» _____ 2025 р.

ЗАВДАННЯ
на курсову роботу
з дисципліни «Проєктування систем кібербезпеки»
студенту Прізвище І. П. групи 1БС-24м

1. Тема: Проєктування засобу для підвищення ефективності захисту файлів, керівник проєкту: Купершетйн Леонід Михайлович, канд. техн. наук, доцент, затверджені протоколом засідання кафедри № 1 від 1 лютого 2024 р.
2. Строк подання студентом роботи 10 червня 2024 р.
3. Вихідні дані до роботи:
   - предметна область – захист файлів;
   - тип захисту – шифрування;
   - операційна система – ОС Windows;
   - математичний апарат – метод DES;
   - тощо.
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити).
   Вступ.
   1 Передпроєктний аналіз системи захисту.
   1.1 Системний аналіз предметної області системи захисту.
   1.2 Формулювання вимог до системи захисту.
   2 Техноробоче проєктування системи захисту.
   2.1 Технічне проєктування системи захисту.
   2.2 Робоче проєктування системи захисту.
   3 Впровадження системи захисту.
   3.1 Проведення випробувань системи захисту.
   3.2 Оцінка ефективності системи захисту.
   Висновки.
   Список використаних джерел.
5. Перелік ілюстративного матеріалу:
   1. Схема роботи. 2. Схема структурна, 3. Алгоритм роботи системи, 4. Схема модулів засобу
6. Дата видачі завдання 11 березня 2024 р.

Студент _____ І. П. Прізвище
Керівник роботи _____ Л. М. Куперштейн

ДОДАТОК В
Приклад анотації

АНОТАЦІЯ

Іванченко А. В. Система захисту файлів методом шифрування: курсова робота з дисципліни «Проєктування систем кібербезпеки».

Дана курсова робота присвячена розробці системи захисту файлів в операційних системах сімейства Windows, методами захисту є шифрування файлів та контроль цілісності за допомогою порівняння геш-значень файлів. У роботі проведено аналіз відомих рішень для захисту файлів, розроблено проєкт системи для забезпечення захисту файлів. Обґрунтовано вибір використовуваних засобів. Реалізовано систему захисту з використанням популярних алгоритмів.

Ключові слова: файл, захист даних, шифрування

ABSTRACT

Ivanchenko A. V. File Protection System Using Encryption Method: A Course project «Cybersecurity Systems Design».

This term paper is dedicated to the development of a file protection system for operating systems of the Windows family. The protection methods used include file encryption and integrity control through comparison of file hash values. The paper analyzes existing solutions for file protection and proposes a system design to ensure file security. The choice of tools used is substantiated, and a protection system has been implemented using popular algorithms.

Keywords: file, data protection, encryption

ДОДАТОК Г
Приклад оформлення змісту

ЗМІСТ

ДОДАТОК Д
Приклад оформлення технічного завдання

Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

ТЕХНІЧНЕ ЗАВДАННЯ
на курсову роботу
«Засіб для захисту інформації на основі візуальної криптографії»

Розробив студент групи 1БС-24м
_____ С. А. Думчиков

Керівник курсової роботи
канд. техн. наук, доц.
_____ Л. М. Куперштейн

«___»_____ 2025 р.

Вінниця 2025 рік

1 Назва та область використання

Засіб для захисту інформації. Область використання: Автоматизовані робочі місця з ОС сімейства Windows з підвищеними вимогами до зберігання секретної інформації.

2 Основа для розробки

Розробка виконується на основі індивідуального завдання, затвердженого протоколом засідання кафедри захисту інформації №12 від 22 лютого 2025.

3 Мета та призначення розробки

Підвищення ефективності захисту даних шляхом застосування візуальної криптографії.

4 Джерела розробки

4.1. Naor, Moni, and Adi Shamir. "Visual cryptography." Workshop on the Theory and Application of of Cryptographic Techniques. Springer Berlin Heidelberg, 1994;

4.2. Verheul, E.R. and H.C.A.van Tilborg. Constructions and properties of k out of n visual secret sharing schemes. Design Codes and Cryptography, 1997. С. 11(2):179–196;

4.3. Cryptographic process and enciphered product URL: https://patents.google.com/patent/US4682954 (дата звернення 11.03.25);

4.4. Liu Feng and Wu ChuanKun. Embedded extended visual cryptography schemes. China, 2006.

5 Вимоги до програмного засобу

5.1 Реалізацію вказаного функціонального профілю буде здійснювати застосована система захисту інформації, яка повинна реалізувати наступні основні функції:

Вимоги до системи захисту в цілому:

– застосунок повинен виконувати захист текстової інформації визначеної довжини;

– система повинна складатися з декількох модулів, які відповідатимуть за створення та розподіл зображень;

– система повинна коректно працювати у визначених умовах;

– система повинна бути простою у використанні для будь-якого користувача;

– система повинна супроводжуватися документацією по правильному застосуванню.

Вимоги до функцій системи:

– система повинна вбудовувати текст у зображення;

– система повинна забезпечувати високу швидкість генерування зображень;

– зображення має не відображати секрет, якщо немає усіх частин, на які було розділено;

– система повинна забезпечити перевірку вхідних даних;

Вимоги до видів забезпечення:

– система повинна працювати на операційних системах Windows 7/8/10;

– система повинна зберігати зображення, створені у ході розподілення секрету.

6 Вимоги до документації

6.1 Документ «Текст програми» ГОСТ 19.401-78.

6.2 Документ «Керівництво користувача» згідно РД 50-34.698-90.

6.3 Документ «Програма та методики випробувань» згідно ГОСТ 19.301-79 або РД 50-34.698.

7 Стадії та етапи розробки

Робота по темі виконується у такі етапи:

Етап	Зміст	Початок	Закінчення
1	Аналіз завдання. Збір матеріалу. Вступ	21.02.25	23.02.25
2	Аналіз літературних джерел, пошук аналогів	24.02.25	30.02.25
3	Системний аналіз предметної області системи захисту	01.03.25	14.03.25
4	Формулювання вимог до системи захисту. Розробка технічного завдання.	15.03.25	28.03.25
5	Розробка технічного проекту системи захисту	29.03.25	18.04.25
6	Розробка робочого проекту системи захисту	19.04.25	09.05.25
7	Випробування системи захисту	10.05.25	23.05.25
8	Оцінка ефективності системи захисту. Аналіз виконання ТЗ. Висновки	24.05.25	02.06.25
9	Оформлення пояснювальної записки. Подання на перевірку	03.06.25	08.06.25
10	Захист курсової роботи	09.06.25	22.06.25

8 Порядок контролю та прийому

До приймання курсової роботи представляється:

– ПЗ до курсової роботи;

– робоча система для реалізації захисту;

– графічні матеріали.

ДОДАТОК Е
Приклад оформлення тексту програми

```
// VisualCryptography : Определяет точку входа для приложения.
// Автор: Stanislav Dumchykov

using System;
using System.Drawing;
using System.Drawing.Imaging;
using System.IO;
using System.Windows.Forms;

namespace VisualCryptography
{
    public partial class FormMain : Form
    {
// Глобальные переменные:
        private Size IMAGE_SIZE = new Size(437, 106); // Текущий размер изображения
        private const int GENERATE_IMAGE_COUNT = 2; // На сколько будет разделено изображение с
секретом

        private Bitmap[] m_EncryptedImages; // Объект класса Bitmap

        public FormMain()
        {
            InitializeComponent();
        }

        private void buttonGenerate_Click(object sender, EventArgs e)
        {
            if (textBoxInput.Text != "")
            {
                if (m_EncryptedImages != null)
                {
                    for (int i = m_EncryptedImages.Length - 1; i > 0; i--)
                    {
                        m_EncryptedImages[i].Dispose();
                    }
                    Array.Clear(m_EncryptedImages, 0, m_EncryptedImages.Length);
                }

                m_EncryptedImages = GenerateImage(textBoxInput.Text);

                panelCanvas.Invalidate();
            }
        }

        private Bitmap[] GenerateImage(string inputText)
        {
            Bitmap finalImage = new Bitmap(IMAGE_SIZE.Width, IMAGE_SIZE.Height);
            Bitmap tempImage = new Bitmap(IMAGE_SIZE.Width / 2, IMAGE_SIZE.Height);
            Bitmap[] image = new Bitmap[GENERATE_IMAGE_COUNT];

            Random rand = new Random();
            SolidBrush brush = new SolidBrush(Color.Black);
            Point mid = new Point(IMAGE_SIZE.Width / 2, IMAGE_SIZE.Height / 2);

            Graphics g = Graphics.FromImage(finalImage);
            Graphics gtemp = Graphics.FromImage(tempImage);

            StringFormat sf = new StringFormat();
            sf.Alignment = StringAlignment.Center;
            sf.LineAlignment = StringAlignment.Center;
            Font font = new Font("Times New Roman", 48);
            Color fontColor;

            g.DrawString(inputText, font, brush, mid, sf);
            gtemp.DrawImage(finalImage, 0, 0, tempImage.Width, tempImage.Height);
```

ДОДАТОК Ж
Приклад оформлення керівництва користувача

Керівництво користувача

1 Вступ

1.1 Галузь використання

Вимоги цього документа застосовуються при:

– попередніх комплексних випробуваннях;

– дослідній експлуатації;

– приймальних випробуваннях;

– експлуатації системи захисту.

1.2 Короткий опис можливостей

Програмний засіб виконує захист секрету текстового вигляду засобами візуальної криптографії для операційної системи Windows. Система містить вбудований модуль, який виконує розподіл частин секрету між учасниками. Система надає можливість явного механічного чи з використанням комп'ютерних засобів відтворення секрету.

1.3 Рівень підготовки користувача

Систему може використовувати користувач, який має досвід роботи з ОС Windows 7, 8, 8.1, 10. Користувач має розуміти, що таке прозорість зображення і чим він відрізняється від білого.

2 Призначення та умови застосування

Система захисту секрету призначена для розміщення секрету на декількох зображеннях з розширенням *.png, що дозволяє захистити інформацію від її відтворення з однієї частини секрету.

Систему варто застосовувати для захисту текстової інформації, факт існування якої треба приховати.

3 Підготовка до роботи

3.1 Склад та зміст дистрибутивного носія

Програмний засіб складається з одного застосунку. Виконуваний файл

VisualCryptography.exe необхідний для запуску програми. У системі повинна бути встановлена платформа .NET Framework.

3.2 Порядок завантаження

Система захисту є портативним засобом, тому для її встановлення достатньо скопіювати виконуваний файл VisualCryptography.exe у робочу директорію, після чого запустити виконуваний файл.

3.3 Порядок перевірки працездатності

При завантажені програмного засобу повинно з’явитися вікно з елементами керування. У разі відсутності вікна програми або появі системних помилок при виконанні програми звертайтесь до розробника за контактними даними.

4 Опис операцій

4.1 Функції і завдання

Засіб захисту текстової інформації виконує наступні функції:

– розміщення секрету на зображенні;

– розподіл зображення з секретом.

Програма працює з текстовою інформацією визначеної довжини та фіксованими розмірами зображення.

4.2 Опис операцій

Завдання: «забезпечення конфіденційності текстової інформації»

Операція: приховування текстової інформації

Умови для виконання операції:

– комп’ютер з ОС Windows 7, 8, 8.1, 10;

– текст.

Підготовчі дії:

Виконати встановлення засобу відповідно до пункту 3.2.

Основні дії:

Запустити файл VisualCryptography.exe. Ввести текст у відповідне поле. Натиснути на кнопку «Згенерувати». Натиснути правою кнопкою миші для

збереження розділених частин зображення з секретом. Дочекатись результату роботи.

5 Аварійні ситуації

У разі збоїв у роботі операційної системи або раптового відключення живлення виконайте перезавантаження робочої станції та розпочніть виконання операції з початку.

Якщо в ході виконання програмного засобу з’являються системні помилки, виконайте перевстановлення засобу відповідно до пункту 3.2.

ДОДАТОК И

Приклад оформлення методики та програми випробувань

Програма та методика випробування

1 Об’єкт випробувань

Об’єктом випробувань є програмний засіб приховування текстової інформації у зображеннях. Програмний засіб призначений для забезпечення конфіденційності текстової інформації.

2 Мета випробувань

Метою проведення випробувань є перевірка надійності функціонування програми, перевірка ефективності захисту, що забезпечує програмний засіб, перевірка новоствореного програмного засобу на наявність помилок та недоліків.

3 Вимоги до програми

Вимоги до системи захисту в цілому:

– система повинна складатися з програмного продукту, який здійснюватиме приховування текстової інформації;

– система повинна виконувати приховувати інформацію будь-якої мови;

– система повинна складатися з одного модуля, який відповідатиме за приховування інформації та розподілу секрету;

– система повинна забезпечувати безпеку при дослідженні;

– система повинна коректно працювати у визначених умовах;

– система повинна бути простою у використанні для будь-якого користувача;

– система повинна супроводжуватися документацією по правильному застосуванню.

Вимоги до функцій системи:

– система повинна здійснювати приховування текстової інформації;

– система повинна здійснювати розподіл зображення з секретом між учасниками;

– система повинна забезпечити захист від дослідження;

– система повинна взаємодіяти з користувачем, попередньо повідомляючи йому проміжні результати роботи та помилки, якщо вони виникали.

Вимоги до програмного забезпечення:

– система повинна працювати на операційних системах Windows 7, 8, 10;

– система повинна розділяти секрет між учасниками, шляхом створення нових зображень;

– система повинна бути доступною для машин з обмеженими обчислювальними ресурсами та застарілим обладнанням;

– система повинна використовувати лише безпечні бібліотеки та алгоритми.

4 Вимоги до програмної документації

Склад програмної документації, пропонованої на випробуванні:

– керівництво користувача (РД 50-34.698-90);

– програма і методика випробувань (ГОСТ 19.301-79);

– текст програми (ГОСТ 19.401-78).

5 Засоби і порядок випробувань:

– виконати статичне дослідження програмного забезпечення;

– провести випробування роботи додатку при використанні тексту будь-якої мови;

– провести випробування роботи додатку при використанні тексту різної довжини;

– перевірити коректність виконання розподілу секрету

ДОДАТОК К

Приклад оформлення списку використаних джерел різного характеру

Посилання на книги (один автор, два автори, три автори):

1. Дробот О. В. Професійна свідомість керівника : навч. посіб. Київ : Талком, 2016. 340 с.
2. Лужецький В. А., Войтович О. П., Дудатьєв А. В. Інформаційна безпека : навч. посіб. Вінниця : УНІВЕРСУМ-Вінниця, 2009. 240 с.

Посилання на книги (чотири автори і більше):

3. Операційне числення : навч. посіб. / С. М. Гребенюк та ін. Запоріжжя : ЗНУ, 2015. 88 с.
4. Основи охорони праці : підручник / О. І. Запорожець та ін. 2-ге вид. Київ : ЦУЛ, 2016. 264 с.
5. Клименко М. І., Панасенко Є. В., Стреляєв Ю. М., Ткаченко І. Г. Варіаційне числення та методи оптимізації : навч. посіб. Запоріжжя : ЗНУ, 2015. 84 с.

Посилання на стандарти:

6. ДСТУ 7152:2010. Оформлення публікацій у журналах і збірниках. [Чинний від 2010-02-18]. Вид. офіц. Київ, 2010. 16 с. (Інформація та документація).
7. ДСТУ 3008:2015. Звіти у сфері науки і техніки. Структура та правила оформлювання. [Чинний від 2017-07-01]. Вид. офіц. Київ : ДП УкрНДНЦ, 2015. 26 с.
8. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні поняття. [Чинний від 1997-01-01]. Вид. офіц. Київ, 1996. 20 с. (Національні стандарти України).

Посилання на авторське свідоцтво:

9. Пат. 43976 Україна, МПК6G01L 7/02. Оптоелектронний пристрій для вимірювання тиску / П. Г. Столярчук, Р. І. Байцар, В. С. Рак, М. П. Гінгін ; власник Нац. ун-т «Львів. політехніка». № 2000105737 ; заявл. 10.10.2000 ; опублік. 15.01.2002, Бюл. № 1.

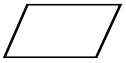
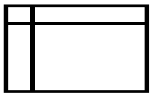
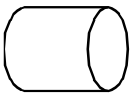
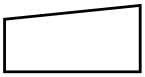
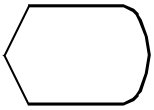
Посилання на електронні джерела:

10. Нові технології розробки вірусів. URL : http://bezpeka.com /news/2008/10/30/virus-injection.html (дата звернення 10.10.2024).
11. Шарая А. А. Принципи державної служби за законодавством України. *Юридичний науковий електронний журнал*. 2017. № 5. С. 115–118. URL: http://lsej.org.ua/5_2017/32.pdf (дата звернення 10.10.2024).

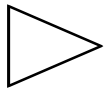
ДОДАТОК Л

Символи даних, процесів і ліній

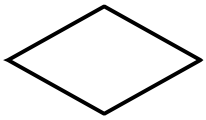
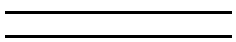
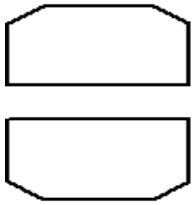
Таблиця Л.1 – Символи даних

Основні символи даних		
Дані		Символ відображає дані, носій даних невизначений
Дані, що запам'ятовуються		Символ відображає дані, що зберігаються, у вигляді, придатному для обробки, носій даних невизначений
Специфічні символи даних		
Оперативний запам'ятовувальний пристрій		Символ відображає дані, що зберігаються в оперативному запам'ятовувальному пристрої
Запам'ятовуючий пристрій послідовного доступу		Символ відображає дані, що зберігаються в запам'ятовувальному пристрої з послідовним доступом (наприклад, магнітна стрічка)
Запам'ятовуючий пристрій з прямим доступом		Символ відображає дані, що зберігаються в запам'ятовувальному пристрої з прямим доступом (наприклад, магнітний диск)
Документ		Символ відображає дані, подані на носії в легкій для читання формі (документ для оптичного або магнітного зчитування, мікрофільм, рулон стрічки з підсумковими даними, бланки даних)
Ручне введення		Символ відображає дані, що вводяться вручну під час оброблення з пристроїв будь-якого типу (клавіатура, перемикачі, кнопки, світлове перо тощо)
Дисплей		Символ відображає дані, подані у візуальній людиночитабельній формі на носії у вигляді пристрою відображення (екран, індикатори введення інформації)

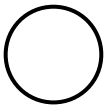
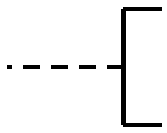
Таблиця Л. 2 – Символи ліній

Основний символ ліній	
Лінія	Символ відображає потік даних або управління. У разі необхідності або для підвищення легкості читання можуть бути додані стрілки-покажчики
Специфічні символи ліній	
Передача управління 	Символ відображає безпосередню передачу управління від одного процесу до іншого. Тип передачі управління повинен бути названий усередині символу (наприклад, запит, виклик, подія)
Канал зв'язку 	Символ відображає передачу даних по каналу зв'язку
Пунктирна лінія	Символ відображає альтернативний зв'язок між двома або більшою кількістю символів, а також використовується для обведення ділянки

Таблиця Л.3 – Символи процесу

Основні символи, процесу		
Процес		Символ відображає функцію обробки даних будь-якого вигляду (виконання певної операції або їх групи, що приводить до зміни значення, форми інформації)
Специфічні символи процесу		
Підпорядкований процес		Символ відображає підпорядкований процес, що складається з однієї або декількох операцій або кроків програми, які визначені у іншому місці
Підготовка для повторювань		Символ відображає модифікацію команди або групи команд з метою дії на деяку подальшу функцію (цикли з параметрами)
Умова або вибір		Символ відображає умову, вибір або функцію типу перемикача, що має один вхід і ряд виходів, і лише один з них може бути активований після обчислення умов усередині цього символу
Паралельні дії		Символ відображає синхронізацію двох або більше паралельних операцій
Межі циклу		Символ, що складається з двох частин, відображає початок і кінець циклу. Обидві частини символу мають один і той самий ідентифікатор. Умови для ініціалізації, прирости, завершення поміщаються усередині символу на початку або в кінці залежно від розташування операції, що перевіряє умову

Таблиця Л.4 – Спеціальні символи

З'єднувач 	Символ відображає вихід в частину схеми і вхід з іншої частини цієї схеми, і використовується для обривання лінії і продовження її у іншому місці. Відповідні символи-з'єднувачі повинні містити одне і те ж унікальне позначення
Термінатор 	Символ відображає вихід в зовнішнє середовище і вхід із зовнішнього середовища (початок або кінець схеми програми, зовнішнє використовування і джерело або пункт призначення даних)
Коментар 	Символ використовують для додавання описових коментарів або записів пояснень з метою пояснення або приміток. Пунктирні лінії в символі коментаря пов'язані з відповідним символом або можуть окреслювати групу символів. Текст коментарів або приміток повинен бути поміщений біля обмежуючої фігури
Пропуск 	Символ (три крапки) використовують в схемах для відображення пропуску символу або групи символів, в яких не визначені ні тип, ні число символів. Символ використовують тільки в символах лінії або між ними. Він застосовується головним чином в схемах, що зображають загальні результати вибору з невідомим числом повторень

Електронне навчальне видання

Леонід Михайлович Куперштейн

Методичні вказівки до виконання курсових робіт з дисципліни «Проєктування систем кібербезпеки» зі спеціальності «Кібербезпека та захист інформації» (освітня програма «Безпека інформаційних і комунікаційних систем»)

Рукопис оформив Л. Куперштейн

Редактор О. Малетіна

Оригінал-макет виготовлено в РВВ ВНТУ

Підписано до видання 17.10.2025
Гарнітура Times New Roman.
Зам. № Р2025-146.

Видавець та виготовлювач
Вінницький національний технічний університет,
Редакційно-видавничий відділ.
ВНТУ, ГНК, к. 114.
Хмельницьке шосе, 95,
м. Вінниця, 21021.
press.vntu.edu.ua;
Email: rvv .vntu@gmail.com
Свідоцтво суб'єкта видавничої справи
серія ДК No 3516 від 01.07.2009 р.