Методичні вказівки

до виконання курсових проектів

з дисципліни

«Захист інформації в інформаційно-комунікаційних системах»

для студентів галузі знань 1701 – Інформаційна безпека
напряму підготовки 6.170101 – Безпека інформаційних і комунікаційних систем

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

Методичні вказівки

до виконання курсових проектів

з дисципліни

«Захист інформації в інформаційно-комунікаційних системах»

для студентів галузі знань 1701 – Інформаційна безпека
напряму підготовки 6.170101 – Безпека інформаційних і комунікаційних систем

Вінниця
ВНТУ
2016

Рекомендовано до друку Методичною радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 3 від 17.11.2016 р.)

Рецензенти:

Ю. В. Булига, кандидат технічних наук, доцент
І. С. Колесник, кандидат технічних наук, доцент

.

Захист інформації в інформаційно-комунікаційних системах: Методичні вказівки, завдання на курсовий проект /Уклад.: О. П. Войтович, Л. М. Куперштейн, В. А. Каплун. - Вінниця : ВНТУ, 2016, - 26 с.

Містять рекомендації з вивчення дисципліни «Захист інформації в інформаційно-комунікаційних системах» та виконання курсового проекту для студентів напряму підготовки «Безпека інформаційних і комунікаційних систем».

ЗМІСТ

1 ТЕМАТИКА ТА ЗМІСТ КУРСОВОГО ПРОЕКТУ

1.1 Тематика

Курсовий проект (КП) – навчальний самостійній проект з дисципліни, яка містить елементи (задачі) навчального, аналітично-розрахункового та науково-дослідницького характеру.

В курсовому проекті з дисципліни «Захист інформації в інформаційно-комунікаційних системах» студент повинен показати знання основних правил побудови захищених інформаційно-комунікаційних систем (ІКС) підприємства та організації. Студент повинен вміти проводити аналіз структури підприємства та його інформаційних потоків, розраховувати можливі ризики на підприємстві, обирати топологію мережі, обґрунтовувати вибір та застосовувати захисні засоби в ІКС підприємства; розраховувати адресацію елементів мережі, обґрунтувати вибір та розраховувати елементи захищеної мережі, обирати методи захисту ІКС, використовувати різні методи сегментації ІКС для забезпечення захисту інформації, налаштовувати централізоване керування програмними та апаратними засобами забезпечення безпеки ІКС, робити висновки щодо ефективності обраних засобів захисту.

Тематика курсового проекту пов’язана з майбутньою спеціальністю студентів. Для програмної реалізації даного курсового проекту пропонуються організувати захищений зв’язок в комп’ютерній мережі, яка складається з окремих підмереж. Вибір структури мережі та організації підмереж обґрунтовуються студентом виходячи зі структури обраного підприємства та варіанта завдання.

Під час виконання курсового проекту студенти повинні використати всі знання, отримані ними під час вивчення дисциплін «Основи інформаційної безпеки», «Прикладана криптологія», «Захист операційних систем», «Засоби програмування», «Організаційне забезпечення інформаційної безпеки підприємства», «Інформаційно-комунікаційні системи», «Захист інформації в інформаційно-комунікаційних системах» як то: аналіз інформаційних потоків підприємства, розробка комп’ютерної мережі, автентифікація в комп’ютерних мережах, протоколи обміну даних, криптографічні протоколи захисту, робота у візуальних середовищах програмування.

Зміст курсового проекту відповідає робочому плану дисципліни «Захист інформації в інформаційно-комунікаційних системах» і повинен відображати суть теми, яка розглядається.

Зміст курсового проекту визначається індивідуальним завданням, яке видається викладачем кожному студенту. Завдання видається не пізніше 6 днів з початку семестру. Курсове проектування включає декілька послідо-

вних етапів, які, в загальному випадку, пов'язані із змістовною постановкою задачі, розробкою індивідуального завдання та технічного завдання, вибором форми представлення задачі, аналізом ІКС підприємства, аудитом інформаційних потоків, вибором оптимального методу рішення, розробка програми безпеки ІКС підприємства, проведенням моделювання та/або дослідження запропонованого методу захисту та формулюванням обґрунтованих висновків щодо отриманих в роботі 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 курсового проекту.

Завдання для курсових проектів визначаються викладачем із загального списку завдань на курсовий проект. Заохочуються пропозиції студентів щодо самостійного, за узгодженням з викладачем, вибору теми курсового проекту поза межами запропонованого в методичних вказівках переліку. Самостійний вибір предметної області, в якій доцільно використовувати сучасні методи захисту ІКС 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 10 семестрі студентам пропонується виконати курсовий проект (КП - 54 годин / 1,5 кредит). Завдання на курсовий проект включає весь матеріал, який було опрацьовано під час лекційних, практичних, лабораторних та самостійних занять протягом курсу вивчення дисципліни.

1.2 Об'єм проекту та його зміст

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

- аналіз ризиків інформаційно-комунікаційної системи підприємства;
- захищена інформаційно-комунікаційна система;
- результати тестування.

2. Розробка повинна бути представлена у вигляді готового працюючого програмного продукту і супроводжуватись пояснювальною запискою, яка б містила в собі такі розділи:

- індивідуальне завдання на курсовий проект;
- аналіз структури підприємства та інформаційних потоків (розмежування доступу);
- обґрунтування вибору методів захисту інформаційно-комунікаційної системи;
- розробку структури захищеної мережі проаналізованого підприємства;

- обґрунтування архітектури сегментів локальної мережі підприємства;
- розрахунок адрес елементів комп'ютерної мережі та вибір комплектуючих до них;
- обґрунтування вибору методів та засобів захисту інформаційно-комунікаційних систем;
- аналіз результатів роботи та тестування при різних вхідних даних;
- висновки та перелік використаної літератури;
- додатки:
    - технічне завдання;
    - схема структурна підприємства;
    - схема інформаційних потоків (матриця доступу);
    - схема мережі підприємства;
    - алгоритм методу захисту;
    - схема роботи програми;
    - лістинг допоміжних модулів.

2 ОФОРМЛЕННЯ ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

2.1 Загальні правила оформлення

При оформленні пояснювальної записки (ПЗ) необхідно дотримуватись вимог до курсового проекту за ГОСТ 2.105-95. Текст пояснювальної записки повинен бути набраний на комп'ютері та роздрукований на принтері.

Обсяг. Обсяг текстової частини визначається кількістю годин СРС, які виділяються для дисципліни на курсовий проект навчальним планом (25-30 с.).

Шрифт і відступи.

Текст ПЗ виконується у відповідності з вимогами ГОСТ 2.105-95 одним із застосовуваних друкувальних та графічних пристроїв виведення ЕОМ з висотою букв і цифр не менше 2,5 мм, (кегль – № 14), через один інтервал (ГОСТ 2.004-88).

Текст пояснювальної записки повинен бути набраний у будь-якому текстовому редакторі шрифтом Times New Roman розміром 14 з інтервалом між рядками 1.

Текст розміщують таким чином, щоб відстань від рамки до робочого поля становила: зліва і справа – 3-5 мм; зверху і знизу – не менше 10 мм; абзац – 5 знаків (відступ 0,75 см). Відступи рамок до країв аркуша: зліва – 20 мм, решта – 5 мм. Наявність рамок у додатках, які містять графічний матеріал, є обов'язковою.

Шрифт та міжрядковий інтервал у додатках можуть бути довільними,

але оформлені так, щоб можна було прочитати і зрозуміти. Відступи: зліва – 2,5 см; справа – 1 см; зверху – 1,5 см; знизу – 2.5 см.

Рамки. На першій сторінці виконується рамка показана у додатку А. Індивідуальне завдання, анотації та додатки (за винятком креслень) виконуються без рамок. Перша сторінка змісту містить рамку 180х40 показану у додатку Б. На інших сторінках ПЗ використовується рамка 180х15 показана у додатку В рис. В1. На кресленнях, що представлені у додатках (схема роботи програми, схема обміну даними, схема функціонування програми, структурна схема тощо) використовується рамка 180х40 показана у додатку В рис. В3.

Нумерація сторінок. Сторінки повинні бути пронумеровані, починаючи з третьої (зміст), у правому нижньому кутку сторінки на рамці. 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 центу 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 необхідно 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, і т.д.). Підрозділи нумерують в межах кожного розділу, пункти – в межах підрозділу і т.д. за формою (3.1, 3.2, 3.2.1, 3.2.2 і т.д.). 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
2	Маршрутизатор	Router0	192.168.0-7.1/24	2C8C.B4B5.8537
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 зі 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 ілюстрацій.

Оформлення рисунків. Розміщують рисунки в тексті або в додатках. В тексті рисунки розміщують симетрично до тексту після першого посилання на неї або на наступній сторінці, якщо на даній вона не уміщується 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 зі 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.

Між рисунком і текстом пропускають один рядок.

Нумерують рисунки в межах розділів або в межах всього документа.

Бажано використовувати засоби автоматичної нумерації рисунків.

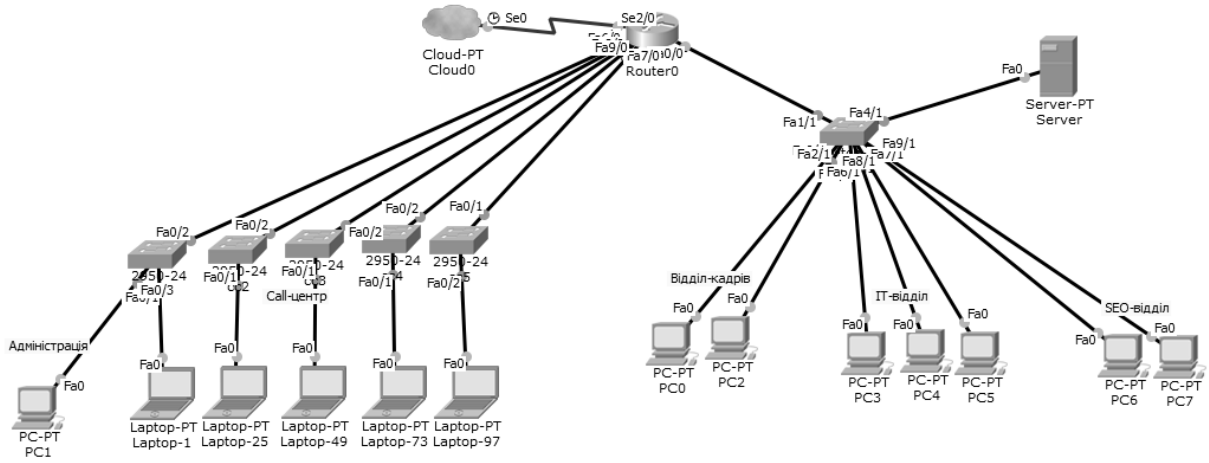


Рисунок 2.1 – Модель ІКС call-центру у програмі Cisco Packet Tracer

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. Для цього після формули ставлять кому і записують пояснення до кожного символу з нового рядка в тій послідовності, в якій вони наведені у формулі, розділяючи крапкою з комою. Перший рядок повинен починатися з абзацу з слова “де” і без будь-якого знака після нього.

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 порядково-

го 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 - 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 курсового проекту, обов'язковими додатками є:

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

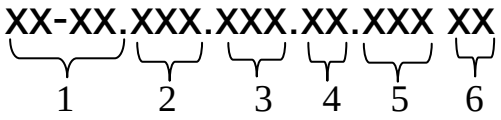
2.3 Вміст вступної частини пояснювальної записки

2.3.1 Титульний аркуш

Титульний аркуш є першою сторінкою КП, яка не нумерується. Згідно з діючим стандартом титульний аркуш виконується за встановленим зразком. Зразок титульного аркушу пропонується у додатку А.

На титульному аркуші для курсових проектів подаються: тема курсового проекту; запис «Пояснювальна записка ...» із зазначенням спеціальності, умовне позначення згідно з прийнятою системою (див. далі); перераховується науковий ступінь та звання керівника. Підписи керівника та студента із зазначенням термінів обов'язкові.

Для курсових проектів доцільною є предметна система умовних позначень, яка має таку структуру:



де 1 (XX-XX) – числовий шифр кафедри, прийнятий у ВНТУ (08-20);

2 (XXX) – умовне скорочення для дисципліни (ЗІвІКС – Захист інформації в інформаційно-комунікаційних систем);

3 (XXX) – перша цифра 0, якщо це проект або 1, якщо робота, друга і третя цифри означають рік, наприклад, 16 – 2016 рік);

4 (XX) – варіант завдання на курсовий проект (наприклад, 01, 02, . . ., 99);

5 (XXX) – перший символ – номер групи (1 або 2), наступні два символи задають номер студента за списком у журналі академічної групи;

6 (XX) – код документа (ПЗ – пояснювальна записка, ТЗ – технічне завдання, ГЧ – графічна частина).

Слід зазначити, що робота, яка подається у вигляді копії, до захисту не приймається.

2.3.2 Індивідуальне завдання

Конкретний зміст кожного КП та етапи виконання визначає керівник на підставі індивідуального завдання, затвердженого завідувачем кафедри не пізніше ніж за два тижні після початку 10 триместру.

Керівник видає індивідуальне завдання до курсового проекту. Індивідуальне завдання в перелік змісту не вноситься та має бути другою сторінкою після титульного аркуша. Зразок індивідуального завдання до курсового проекту наведено в додатку Г.

Керівник проекту пропонує зміст пояснювальної записки, в навчальних цілях зміст може висвітлюватись в індивідуальному завданні.

В залежності від специфіки дисципліни керівник курсового проекту може пропонувати тему, яка вимагає конкретного обґрунтування та розробки індивідуального завдання. Індивідуальне завдання до курсового проекту повинно містити термін видачі, підписи керівника та студента.

Індивідуальне завдання на курсовий проект 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 курсового проекту. Анотація повинна коротко характеризувати мету роботи, за-

соби, використанні для досягнення поставленої задачі, коротку інформацію про досягнуті результати. Розмір анотації повинен становити приблизно 1/3 частину сторінки. Анотація повинна бути двома мовами українською та англійською.

Анотацію розміщують безпосередньо за аркушем з індивідуальним завданням, починаючи з нової сторінки (третьої), нумерація якої не зазначається. Приклад анотації наведений у додатку Д.

2.3.4 Зміст

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

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

Приклад оформлення змісту можна бачити у додатку Е.

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

Вступ висвітлює:

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

Кількість сторінок вступу не повинна перевищувати 2 сторінки.

2.4.2 Предпроектний аналіз структури підприємства та ризиків

Проводиться загальний аналіз структури підприємства та його інформаційно-комунікаційної системи. Аналізується загальна кількість працівників, відділів, вузлів та їх взаємодія. Наводиться структурна схема підприємства з указанням всіх відділів та працівників, які в них працюють, їх посади та функціональні обов'язки пов'язані з використанням інформаційних технологій та комп'ютерних мереж. Наводиться схема інформаційно-комунікаційної системи підприємства з указанням IP-адрес мережевих вузлів. Обов'язково наводиться таблиця з описом мережевого обладнання, що використовується для інформаційного обміну.

Проводиться аналіз інформаційних потоків, які існують в інформаційно-комунікаційній системі підприємства. Окремо виділяються зовнішні та внутрішні потоки, а також інформаційні потоки, які використовуються для обміну даними між різними відділами підприємства. На структурній схемі необхідно показати окремі потоки інформації, що, відповідно до законодавства чи внутрішніх інструкції потребують захисту. Визначаються класи інформації за цілісністю, доступністю, конфіденційністю та спостережністю (табл. 2.2).

Таблиця 2.2 – Модель класифікації інформації.

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

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

Таблиця 2.3 – Інформація, що підлягає захисту

№	Вид	Ознаки КІ	Роль	Вид	Ресурс
1	бази персональних даних працівників	Ц1, Д2, К0	Директор, відділ кадрів	Внутрішня	РС0, РС2

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

В підрозділі Аналіз ризиків та методів захисту ІКС підприємства відповідно до структури підприємства, описаної в підрозділі 1.1, повинні бути детально оцінені ризики інформації, що циркулює в мережі підприємства,

та методи захисту мереж з посиланням на відповідні літературні джерела. Необхідно навести таблицю, в якій зазначити загрозу, ймовірність виникнення, вартість реалізації та оцінку ризику.

Навести та описати декілька варіантів організації захищеної мережі підприємства. Обрати найбільш перспективний напрямок та зробити обґрунтування вибору.

В цьому розділі формуються основні вимоги до апаратних та програмних показників системи, яка розробляється для поставленої задачі, послідовність основних кроків, необхідних для створення захищеної мережі підприємства. Якщо використовуються якісь особливі методи або логічні рішення поставленої задачі, їх теж потрібно описати.

Наприклад, якщо на підприємстві використовуються бездротові технології за стандартом 802.11, то необхідно сформулювати такі правила:

- виділити всі бездротові точки доступу у окрему підмережу, яка не містить інші ресурси організації. DHCP-сервер призначає імена користувачам бездротової мережі;
- всі бездротові засоби, які підключають до корпоративної мережі повинні бути довіреними (тобто пройти попередню реєстрацію). Користувачі повинні проходити процедуру автентифікації та авторизації при кожному приєднанні до бездротової мережі;
- для забезпечення конфіденційності даних – рекомендується використовувати VPN;
- …..

Даний розділ має бути змістовним, конкретним, зрозумілим, оскільки саме він демонструє знання та навички у галузі аналізу безпеки підприємства. Рекомендований обсяг підрозділу – 5-8 сторінок пояснювальної записки.

2.4.3 Вимоги безпеки ІКС

Залежно від того, які ризики є найбільш значимими для інформаційно-комунікаційної системи підприємства та індивідуального завдання обираються вимоги до методів захисту на основі.

1) Сегментація мережі на основі автентифікація користувачів на сервері.

2) Сегментація мережі на основі технології VLAN. користувачів на сервері.

3) Сегментація мережі на основі технології VPN.

4) Сегментація мережі на основі технології міжмережевих екранів.

5) Сегментація мережі на основі хмарних технологій.

6) Інші методи.

Описуються переваги та недоліки обраного підходу та необхідність використання саме такого методу.

При викладенні тексту ПЗ забороняється переписування матеріалів лі-

тературних джерел, сканування рисунків, які мають відношення до основної частини. Частину описового матеріалу (у вигляді таблиць, рисунків, графічної інформації) бажано виносити у додатки до пояснювальної записки, а у тексті посилатись на ці додатки.

У випадку, якщо результатом курсового проекту повинен бути програмний продукт, окремими підпунктами бажано описати розробку загальної схеми функціонування програми або схему роботи програми. Для окремих модулів, що входитимуть до складу програмного засобу, необхідно розробити блок-схеми алгоритмів, структурні схеми з наведенням основних блоків, покрокове викладення алгоритму з розгалуженням і т. ін.

У випадку, якщо курсовий проект присвячений дослідженню методів захисту, необхідно навести алгоритм дослідження, схему зв'язків між частинами інформаційного наповнення, схеми подання матеріалу, схеми даних, таблиці з основними характеристиками і функціональними особливостями досліджуваних об'єктів, порівняльними характеристиками, перевагами та недоліками і т. д.

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

Відповідно до обраного методу обґрунтовується використання тих чи інших засобів захисту, що відповідають цьому методу. Обрані засоби повинні бути конкретними програмними або апаратними рішеннями, які можна використовувати у корпоративних мережах, з врахуванням економічної доцільності їх використання. Недостатньо описати один засіб і зазначити, що він найкращій. Як результат навести таблиці порівняння різних методів та критерії за якими обрані необхідні засоби захисту інформаційно-комунікаційної системи. Навести схеми взаємодії, які притаманні цим засобам захисту, наприклад схему автентифікації користувача у файловому сервері, або схему організацію віртуальної приватної мережі з вказанням всіх мережевих взаємодій.

Вказати правила, за яким має відбуватись реалізація методу захисту, наприклад, матрицю доступу для віртуальної локальної мережі чи загальні правила для міжмережевого екранування. Наприклад

Для забезпечення нормального функціонування мережі необхідно:

– заборонити широкомовні адреси;
– заборонити використання всіх портів для обміну TCP/UDP;
– обмежити смугу пропускання;
– проводити аудит вхідного та вихідного трафіку;
– відкрити порт 80 (tcp) для роботи робочого місця веб-оператора;
– ….

Рекомендується навести запропоновані рішення у вигляді таблиць. Приклад правил для міжмережевого екранування наведений у табл. 2.4.

Таблиця 2.4 – Правила для міжмережевого екранування

Номер правила	IP-адреса відправника	IP-адреса одержувача	Служба	Дія
1	Any	Поштовий сервер	SMTP	Accept
2	Any	Веб-сервер	HTTP, HTTPS, FTP, SSH	Accept
3	Поштовий сервер	Any	SMTP	Accept
4	ПК з внутрішньої мережі	Any	HTTP, HTTPS, FTP, telnet, SSH	Accept
5	Внутрішній DNS	Any	DNS	Accept
6	Any	Any	Any	Deny

Підрозділ повинен бути описово-обґрунтувальний і займати приблизно 8-10 сторінок ПЗ.

2.4.4 Сегментація мережі

Цей розділ повинен бути присвячений розробці захищеної ІКС та рекомендацій по роботі з нею.

Обґрунтовуються з точки зору доцільності та наводиться топологія загальної мережі підприємства та зв’язки між підмережами. Окремо обґрунтовуються та наводяться у вигляді структурних схем топології підмереж підприємства у відповідності до таких критеріїв: кількість працівників, що потребують роботи в локальній чи глобальній мережі, методи захисту, які будуть застосовуватись, до інформації, що циркулює в мережі, обрані методи сегментації.

Вказуються мережеві вузли (комп’ютери користувачів, сервери віддалені ресурси), на яких буде оброблюватись інформація, що потребує захисту. Показують шляхи, якими буде передаватись інформація, що потребує захисту.

В цьому розділі необхідно розробити структурну схему мережі підприємства та промоделювати її роботу за допомогою пакету програм Packet Tracer (або іншого пакету прикладних програм призначених для моделювання мереж).

Можлива зміна попередньої топології інформаційно-комунікаційної системи, в такому випадку обґрунтовується вибір класу мережі, розраховуються маски підмереж змінної чи постійної довжини, виділяються IP-адреси для конкретних мережевих вузлів, які підключені, чи можуть бути підключені до мережі.

У випадку апаратної реалізації розробляється система захисту з використанням обраних апаратних засобів. Надається функціональна схема ро-

боти системи захисту. Описуються налаштування щодо захисту. Модулюється її функціонування в різних режимах.

У випадку програмно-апаратної реалізації розробляється програма для забезпечення захисту інформації в комп'ютерній мережі. В тексті пояснювальної записки наводяться основні функції, які реалізують поставлену мету та їх коротке обґрунтування і опис. Наводяться рисунки з графічним інтерфейсом користувача (або консолі), приклади тестування програми на різних IP-адресах тощо.

Наводяться налаштування засобів захисту, що були обрані у другому розділі. Реалізуються конкретні методи автентифікації, налаштовуються конкретні засоби. Обов'язково показати скріншоти з налаштованими механізмами безпеки. В середовищах моделювання (за потребою) показана взаємодія мережевих вузлів та захищені інформаційні потоки.

Приклад:

Необхідно створити VLAN на комутаторі Switch2. Для цього необхідно написати в консолі комутатора:

```
Switch(config)#vlan 10
Switch(config-vlan)#name VkadrivN10
```

Далі потрібно призначити VLAN для кожного порту, до якого підключені комп'ютери відділу основного виробництва:

```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport access vlan 10
Switch(config)#interface FastEthernet2/1
Switch(config-if)#switchport access vlan 10
```

Комп'ютери, що не входять до VLAN1, але приєднані до комутатора Switch1 (рис. 3.10).

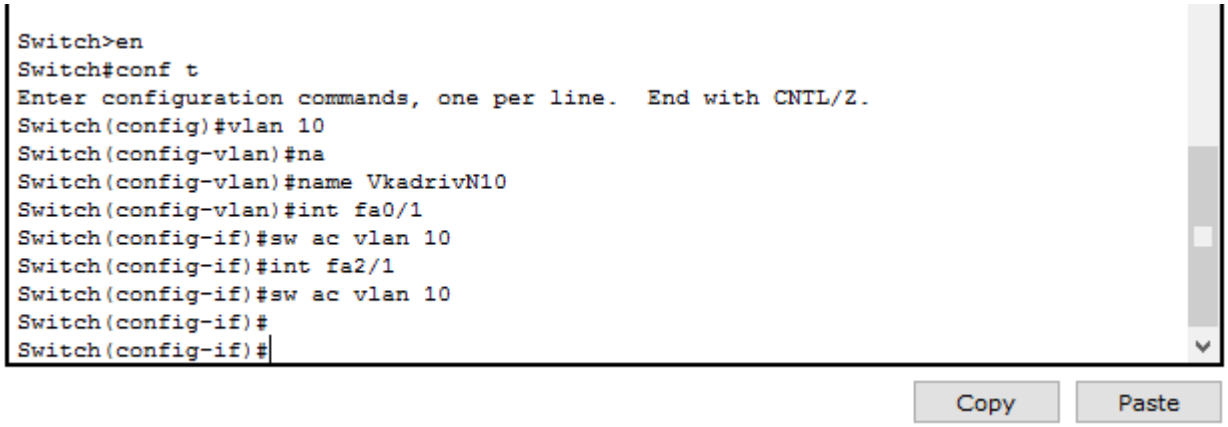


Рисунок 3.10 – Створення першої VLAN на комутаторі Switch1

Обов'язковим є тестування обраних методів та засобів захисту, за допомогою якого можна довести ефективність запропонованих рішень. Ре-

комендовано навести переоцінювання ризиків, в якому підтвердити (чи спростувати) ефективність запропонованих рішень.

Приклад:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	PC2	ICMP		0.000	N	0
	Successful	PC2	PC0	ICMP		0.000	N	1
	Failed	PC2	PC3	ICMP		0.000	N	2

Рисунок 3.11 – Перевірка роботи VLAN1

Цей розділ є практичної направленості і може містити від 8 до 10 сторінок.

2.5 Висновки

Висновки оформляють з нової пронумерованої сторінки посередині великими літерами більш високої насиченості.

У висновках приводяться основні результати роботи над курсовим проектом. На основі результатів роботи надаються обґрунтовані висновки щодо переваг та недоліків застосування того чи іншого рішення. Наводяться недоліки та переваги розробленої , труднощі при розробці та причини, що їх обумовили і можливі шляхи їх подолання, можливі рекомендації прикладного застосування та шляхами (перспективами) удосконалення розробленої захищеної мережі підприємства чи організації.

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 ГОСТ 7.1:2006 «Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання», перелік літературних джерел, які було використано в процесі виконання проекту, і на яку є посилання в тексті пояснювальної записки. Кожне джерело повинно бути вказано разом з видавництвом, роком видання, кількістю сторінок. Літературу записують мовою оригіналу. В списку кожне джерело записують з абзацу, нумерують арабськими цифрами, починаючи з одиниці.

Якщо у списку використаних джерел є посилання на Інтернет-сторінки, слід наводити і їх.

Приклад оформлення списку використаних джерел можна переглянути у списку використаних джерел у цих методичних вказівках.

2.7 Додатки

Обов'язковим додатком є технічне завдання (Додаток А). Технічне завдання розробляється студентом самостійно на основі індивідуального завдання протягом 2-х перших тижнів триместру. Зразок технічного завдання наведено у додатку Ж.

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 і т.д., що пояснюють наведений текст.

Кожен додаток необхідно починати з нової сторінки, вказуючи зверху посередині рядка слово "Додаток" і через пропуск – його позначення. Додатки позначають послідовно великими українськими буквами, за винятком букв Г, Є, З, І, Ї, Й, О, Ч, Ь, наприклад, Додаток А, Додаток Б і т.д. Якщо додатків більше ніж букв, то продовжують позначати арабськими цифрами. Дозволяється позначати додатки латинськими буквами, за винятком букв *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 ОФОРМЕЛЕННЯ ГРАФІЧНОЇ ЧАСТИНИ

Як результат виконання курсового проекту є розробка графічної частини, яка демонструє основні результати виконаної розробки.

В курсовому проекті обов'язковими є два креслення:

1) Схема роботи обраного методу захисту,
2) Схема структурна захищеної ІКС підприємства,

Креслення друкуються на аркушах формату А4 з рамками 40х180 мм, як показано у додатку В.2. Графічна частина прикріпляється до пояснювальної записки, але не є її складовою частиною.

Графічна частина має окрему нумерацію та підписи у рамках.

4 ГРАФІК ВИКОНАННЯ КУРСОВОГО ПРОЕКТУ І ПОРЯДОК ЙОГО ЗАХИСТУ

Рекомендується такий графік виконання курсового проекту (табл. 4.1), який враховує самостійну роботу студентів під час 10-го триместру (16 тижнів).

Таблиця 4.1 - Графік виконання курсового проекту

Зміст розділу	Термін виконання
Отримання завдання на курсову роботу, розробка і оформлення технічного завдання	1-2 тижд.
Розробка структури підприємства, з'ясування які відділи за яку інформацію відповідають, аналіз інформаційних потоків підприємства, з виділенням, тих які потребують захисту; формування карти інформаційних ресурсів, розробка матриці доступу.	3-4 тижд.
Аналіз та обґрунтування вибору методів захисту комп'ютерної мережі підприємства. Вибір реалізації системи захист.	5-6 тижд.
Обґрунтування та розробка топології комп'ютерної мережі підприємства розбиття на підмережі, виділення адрес IP та розрахунок масок під ме-	6-8 тижд.
Вибір та обґрунтування вибору методів захисту інформації відповідно до обраної реалізації. Представлення алгоритму роботи та його детальний	9-10 тижд.
Сегментування ІКС, яке реалізує обраний метод та організацію захищеного зв'язку відповідно до проаналізованих інформаційних потоків.	11-13 тижд.
Оформлення пояснювальної записки до курсового проекту, розробка рекомендацій по роботі з розробленим методом захисту.	13-14 тижд.
Здача курсового проекту на попередню перевірку: демонстрація роботи програми та чернетки пояснювальної записки (можливий її електронний варіант)	15 тижд.
Корегування і доповнення (при необхідності) згідно зауважень керівника курсового проекту, врахування і виправлення пояснювальної записки.	15 тижд.
Захист курсового проекту.	16 тижд.

Готовність до захисту курсового проекту визначає керівник за результатами попередньої перевірки якості пояснювальної записки та дієздатності захисту. Записка повинна бути здана керівнику на перевірку не менш, як за тиждень до визначеного терміну захисту проекту. Якщо робота виконана в повному обсязі і не має принципових помилок, керівник допускає студента до захисту. В іншому випадку проект повертається студенту на доопрацювання. Після позитивного висновку про готовність курсового проекту студент повинен захистити його перед комісією у складі двох викладачів, які призначені кафедрою.

5 ОЦІНЮВАННЯ КУРСОВОГО ПРОЕКТУ

Оцінюється курсовий проект членами комісії після її захисту студентом у балах і за національною шкалою оцінок. Загальна кількість балів включає (табл. 5.1) оцінки змісту роботи (до 34 балів), оформлення (до 20 балів), графічної частини (до 20 балів) та захисту (до 26 балів).

Таблиця 5.1 - Оцінювання курсового проекту

Розробка	Пояснювальна записка	Графічна частина	Захист	Всього
34	20	20	26	100

При оцінюванні курсової роботи за кредитно-модульною системою враховуються

- кваліфікаційний рівень (фаховість, дотримання стандартів) підготовки захисту ІКС;
- обґрунтування актуальності теми, на яку підготовлено курсовий проект;
- 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 курсового проектування.

Підготовка курсового проекту – сумарно 100 балів, у тому числі:

Якість розробки проекту – 34 бали:

- фахова вмотивованість рішень – 10 бали;
- логічність і послідовність рішень – 10 балів;
- обґрунтованість та оптимальність обраних рішень – 10 балів;
- дотримання стандартів побудови систем захисту – 4 бали.

Зміст пояснювальної записки – 20 балів:

- відповідність структурних розділів визначеній тематиці та вимогам до даного типу робіт: *вступ; основна частина; висновки; додатки – 10* балів.
- відповідність оформлення ПЗ стандартам –5 балів;
- наявність посилань та списку використаних джерел – 3 бали;
- дотримання граматичних і стилістичних правил – 2 бали.

Зміст графічної частини – 20 балів:

- відповідність графічної частини завданню – 8 балів;
- відповідність графічної частини тексту пояснювальної записки –7 балів;
- відповідність графічної частини стандартам –5 балів.

Захист курсового проекту – 26 балів:

- вміння студента логічно структурувати доповідь та доводити до присутніх у стислій формі основні результати – 13 балів;
- відповіді на запитання (чіткість формулювання та відповідність запитанню) – 13 балів.

Таблиця 5.2 - Складники оцінки курсового проекту за кредитно-модульною системою

Вид роботи	Кількість балів
фахова вмотивованість рішень	10
логічність і послідовність рішень	10
обґрунтованість та оптимальність обраних рішень	10
дотримання стандартів побудови систем захисту	4
відповідність структурних розділів визначеній тематиці та вимогам до даного типу робіт: вступ; основна частина; висновки; додатки	10
відповідність оформлення ПЗ стандартам	5
наявність посилань	3
дотримання граматичних і стилістичних правил	2
відповідність графічної частини завданню	8
відповідність графічної частини тексту ПЗ	7
відповідність графічної частини стандартам	5
вміння студента логічно структурувати доповідь та доводити до присутніх у стислій формі основні результати	13
відповіді на запитання (чіткість формулювання та відповідність запитанню)	13
Загальна кількість балів	100

Для переведення суми балів в оцінку за національною шкалою використовуємо шкалу оцінювання (таблиця 5.2).

Таблиця 5.3 - Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
		курсового проекту
90 – 100	**A**	відмінно
82-89	**B**	добре
75-81	**C**	
64-74	**D**	задовільно
60-63	**E**	
35-59	**FX**	незадовільно з можливістю повторного складання
0-34	**F**	незадовільно з обов’язковим повторним вивченням дисципліни

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 за напрямом курсового проекту.

6 ВАРІАНТИ ЗАВДАНЬ

Варіанти підприємства обираються відповідно до номера у журналі академічної групи або студент пропонує своє. Наприклад, студент Інжиєвський А. В. записаний в журналі під 5-им номером та пише курсову у 2016 р., отже він має розробити захист Букмекерської контори.

Варіант підприємства

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

7 ЛІТЕРАТУРА

1. Закон України «Про інформацію» : *за станом на 1 січня 2016 р.* / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» : *за станом на 1 січня 2016 р.* / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=80%2F94-%E2%F0

3. Лужецький В. А. Основи інформаційної безпеки. Навчальний посібник [рекомендований МОН] / Лужецький В. А., Войтович О. П., Кожухівський В. Д. – Вінниця ВНТУ, 2013. – 246 с.

4. Дудатьєв А. В. Захист комп'ютерних мереж. Теорія та практика. Навчальний посібник / Дудатьєв А. В., Войтович О. П., Каплун В. А. – Вінниця ВНТУ, 2010. – 219 с.

5. Лужецький В. А. Захист персональних даних. Навчальний посібник / Лужецький В. А., Войтович О. П., Дудатьєв А. В. – Вінниця ВНТУ, 2009. – 240 с.

6. Тимошенко А. А. Защита информации в специализированных информационно-телекоммуникационных системах : Конспект лекцій / А. А. Тимошенко, - Киев: НТУУ "КПИ", ФТИ, 2010. – 252 с.

7. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Вид.група BUV, 2009. – 608 с.

8. Смит Р. Э. Аутентификация: от паролей до открытых ключем / Р. Э. Смит. – М.: «Вильямс», 2002 – 432 с.

9. Гордейчик С. В. Безопасность беспроводных сетей / С. В. Гордейчик, В. В. Дубровин. – М. : Горячая линия-Телеком, 2008. – 288 с.

10. Защита информации в телекоммуникационных системах / Г. Ф. Конахович, В. П. Климчук, С. М. Паук. – К.: «МК-Пресс», 2005. – 288 с.

11. Есин В. И. Безопасность информационных систем и технологий / В. И. Есин, А. А. Кузнецов, Л. С. Сорока. – Х. : ООО «ЭДЭНА», 2010. – 656 с.

12. Разрушающие программные воздействия: Учебно-методическое пособие / [А. Б. Вавренюк, Н. П. Васильев, Е. В. Вельмякина и др.; под ред. М. А. Иванова.] – М. : НИЯУ МИФИ, 2011. – 328 с.

13. Информационная безопасность открытых систем : Учебник для вузов. В 2-х томах. Том 2 – Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. – М.: Горячая линия-Телеком, 2008. – 558 с.

14. Unix и Linux. Руководство системного администратора / [Эви Немет, Гарт Снайдер, Трент Хейн, Бэн Уэйли]. - Вильямс, 2012. – 1312 с.

15. Межсетевые экраны : учеб. пособие / А. М. Суровов [и др.]. - М. : Рудомино, 2011. - 290 с.

16. Таненбаум Э. Современные операционные системы / Э. Таненбаум. – 3-е изд. – СПб.:Питер, 2010. – 1120 с.: ил. – ISBN 978-5-49807-306-4.

17. Бэндл Д. Защита и безопасность в сетях Linux. Для профессионалов / Д. Бэндл. – СПб.: Питер, 2002. – 480 с.: ил. – ISBN 5-318-00057-6.

18. Роб П. Системы баз данных: проектирование, реализация и управление. / П. Роб, К. Коронел. - СПб.: БХВ-Петербург, 2004. – 1040 с.

19. Захист інформації. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2-97. – [Чинний від 1998 – 01 - 01]. – К.: Держспоживстандарт України, 2006. – 45 с.

20. Типове положення про службу захисту інформації в автоматизованій системі : НД ТЗІ 1.4-001-2000. – [Затверджений наказом ДСТСЗІ СБ України від 04.12.2000 р. № 53]. – К.: ДСТСЗІ СБ України, 2000. – 51 с.

21. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-003-99. – [Затверджений наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22]. – К.: ДСТСЗІ СБ України, 1999. – 38 с.

22. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-002-99. – [Затверджений наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22]. – К.: ДСТСЗІ СБ України, 1999. – 41 с.

23. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 2.5-004-99. – [Затверджений наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22]. – К.: ДСТСЗІ СБ України, 1999. – 56 с.

24. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу : НД ТЗІ 2.5-005-99. – [Затверджений наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22]. – К.: ДСТСЗІ СБ України, 1999. – 36 с.

25. Бармен С. Разработка правил информационной безопасности : [пер. с англ.] / Скотт Бармен – М. : «Вільямс», 2002. – 208 с. – ISBN: 5-8459-0323-8

ДОДАТКИ

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

КУРСОВИЙ ПРОЕКТ
з дисципліни «Захист інформації в інформаційно-комунікаційних системах»
на тему: «Захист інформаційно-комунікаційної системи підприємства»
08-20.ЗІвІКС.015.01.101 ПЗ

Студента 4 курсу БС-14 (МС) групи
напряму підготовки 6.170101 - Безпека інформаційних і комунікаційних систем
Прізвище І. П.
(прізвище та ініціали)
Керівник к.т.н., доцент
Войтович О. П.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Національна шкала _____
Кількість балів: _____ Оцінка: ECTS _____

Члени комісії:

_____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

м. Вінниця – 2015 рік

Інв. | Підпис та да- | На зам. | Інв. № | Підпис та дата

Додаток Б
Приклад рамки на першу сторінку змісту

					08-20.ЗІВІКС.015.01.101 ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Прізвище І. П.			Захист інформаційно-комунікаційної системи підприємства. Пояснювальна записка	Літ.	Арк. 3 / Аркушів 26
Перевір.		Войтович О.П					
Реценз.						ВНТУ, гр. БС-14МС	
Н. Контр.		Войтович О.П.					
Затверд.		Лужецький В.А.					

Додаток В
Приклади рамок

Рисунок В.1 - Рамка на основну частину пояснювальної записки (180х15 мм)

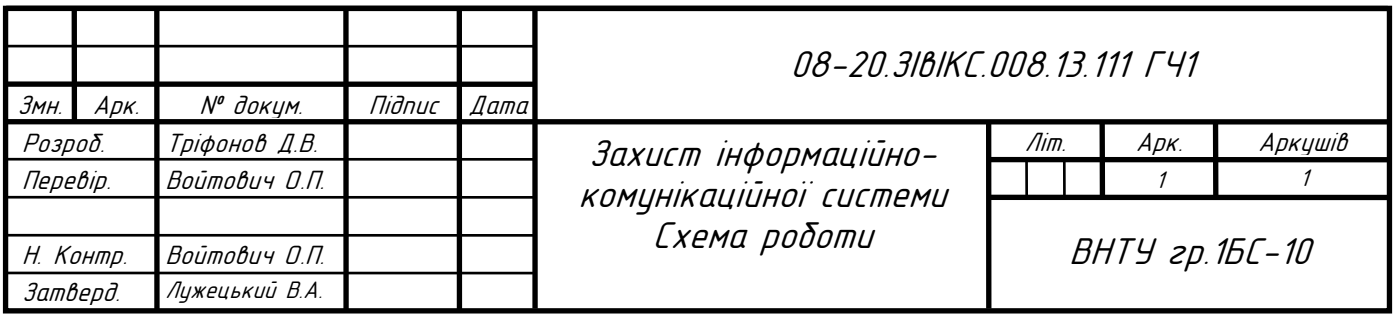


Рисунок В.2 - Рамка на креслення у графічній частині (180х40 мм)

Додаток Г
Приклад оформлення індивідуального завдання

Вінницький національний технічний університет
Факультет Інформаційних технологій та комп'ютерної інженерії
Кафедра Захисту інформації
Освітньо-кваліфікаційний рівень бакалавр
Напрям підготовки 6.170101 – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Зав. кафедри ЗІ, д.т.н., проф.
_____В.А. Лужецький
(підпис)
"___" _____ 2015 р.

ЗАВДАННЯ
на курсовий проект
з дисципліни "Захист інформації в інформаційно-комунікаційних системах"
студенту Прізвище І. П. групи 1БС-12б

1. Тема роботи: Захист інформаційно-комунікаційної системи підприємства
керівник проекту: Войтович Олеся Петрівна, к. т. н., доцент,
затверджені протоколом засідання кафедри № 1 від 1 вересня 2015 року
2. Строк подання студентом роботи 1 грудня 2015 р.
3. Вихідні дані до роботи:
   - Підприємство – Підприємство;
   - Сегменти, що потребують захисту – Сегмент, що потребує захисту;
   - Автентифікація – метод автентифікації;
   - Примітка - примітка.
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
   Вступ.
   1. Предпроектний аналіз інформаційно-комунікаційної системи та ризиків.
   2. Розробка вимог безпеки, що включає такі питання захисту мережі:
      - автентифікація;
      - віртуальна локальна мережа;
      - міжмережеве екранування;
      - віддалені користувачі;
      - хмарні застосунки.
   3. Сегментація мережі (вибір, налаштування та тестування програмно-технічних засобів).
   Висновки.
   Список використаних джерел.
   Додатки.
5. Перелік графічного матеріалу
   1. Захист інформаційно-комунікаційної системи. Схема роботи (Креслення А4)
   2. Захищена інформаційно-комунікаційна система. Схема структурна (Креслення А4)
6 Дата видачі завдання 11 вересня 2015

Студент **_____ Прізвище І. П.**
Керівник роботи **_____ Войтович О. П.**

Додаток Д
Приклад анотації

АНОТАЦІЯ

УДК 681.325.5

Петренко І. М. Захист інформаційно-комунікаційної системи підприємства. Курсовий проект – Вінниця: ВНТУ, 2013, - 35с.

Українською мовою. Рисунків 7, таблиць 2, бібліографій 12.

Курсовий проект присвячений розробці захисту інформаційно-комунікаційної системи ТОВ „Агроград В”, для реалізації і впровадження якої було запропоновано та промодельовано сегментовану на базі списків ACL інформаційно-комунікаційну систему відповідно до проаналізованих загроз підприємства ТОВ „Агроград В”.

ABSTRACT

Petrenko I. M. Enterprise data network system protection. Course project – Vinnitsya: VNTU, 2013, - 35 c.

Ukrainian. Figures 7, tables 2, literature 12.

Course project is dedicated to developing a computer network security system of Ahrohrad V, for the realization and implementation of which data network system segmentation based on ACL it is designed.

Додаток Е
Приклад змісту

ЗМІСТ

Додаток Ж
Приклад технічного завдання

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

ТЕХНІЧНЕ ЗАВДАННЯ
до курсового проекту на тему
«Захист інформаційно-комунікаційної системи підприємства»
08-20.ЗІвІКС.008.13.116 ТЗ

Керівник курсового проекту
к. т. н., доц.
_____ О. П. Войтович

"____" _____ 2016 р.

Вінниця 2016

1 Назва та область використання

Захист інформаційно-комунікаційної системи підприємства. Область використання: захист інформаційних ресурсів підприємства.

2 Основа для розробки

Розробка виконується на основі індивідуального завдання, затвердженого протоколом засідання кафедри захисту інформації №1 від 11.09.16.

3 Мета та призначення розробки

Підвищення ефективності захисту даних, що передаються мережею підприємства за допомогою автентифікації.

4 Джерела розробки

4.1. Дудатьєв А. В. Захист комп'ютерних мереж. Теорія та практика. Навчальний посібник / Дудатьєв А. В., **Войтович О. П.**, Каплун В. А. – Вінниця ВНТУ, 2010. – 219 с.

4.2. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд./ В. Г. Олифер, Н. А. Олифер – СПБ.: ПИТЕР, 2007. – 958 с.

4.3. Тимошенко А. А. Защита информации в специализированных информационно-коммуникационных системах: Текст лекций/ Тимошенко А.А./ НТУУ «КПІ», 2010. – 252 с.

4.4. Хогдал Дж. Анализ и діагностика компьютерных сетей./ Дж. Хогдал – К. : Компьютерная литература, 2010 – 120с.

4.5. Столлингс В. Основы защиты сетей. Приложения и стандарты/ Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002. — С. 432.

5 Вимоги до захисту інформації

1.1 Підприємство – Провайдер Інтернет-послуг.

1.2 Сегменти, що потребують захисту – відділ адміністурвання;

1.3 Автентифікація – джерела змін у налаштуваннях;

1.4 Примітка - висока доступність послуг.

1.5 Протоколи – RADIUS.

6 Вимоги до документації

6.1 Програмна документація повинна бути оформлена згідно ГОСТ 19.105-78 «Общие требования к программным документам».

7 Стадії та етапи розробки

Робота по темі виконується у такі етапи:

Етап	Зміст	Початок	Закінчення	Примітка
1	Аналіз завдання. Вступ	11.09.16	13.09.16	
2	Розробка технічного завдання	13.09.16	18.09.16	
3	Аналіз структури магазину та його інформаційних ресурсів	18.09.16	25.09.16	
4	Аналіз загроз інформаційно-комунікаційної системи магазину	25.09.16	02.10.16	
5	Вибір та обґрунтування методу захисту	02.10.16	09.10.16	
6	Розробка програми безпеки інформаційно-комунікаційної мережі	09.10.16	16.10.16	
7	Виконання захисту мережі	16.10.16	30.10.16	
8	Розробка графічної частини	30.10.16	06.11.16	
9	Аналіз виконання ТЗ, висновки	06.11.16	09.11.16	
10	Оформлення пояснювальної записки	09.11.16	11.29.16	
11	Подання на перевірку	19.12.2016		
12	Захист курсового проекту	20.12.2016		

8 Порядок контролю та прийому

До приймання курсового проекту представляється :

- ПЗ до курсового проекту;
- робоча система для реалізації захисту;
- графічні матеріали.

Початок розробки
11.09.2016.
Крайній термін виконання курсового проекту
24.12.2016.

Розробив студент групи 1БС-12б _____ Мідзяєв В.С.

Навчальне видання

Методичні вказівки
до виконання курсових проектів
з дисципліни
«Захист інформації в інформаційно-комунікаційних системах»
для студентів галузі знань 1701 – Інформаційна безпека
напряму підготовки 6.170101 – Безпека інформаційних і комунікаційних систем

Редактор В. Дружиніна

Укладачі: Войтович Олеся Петрівна
Куперштейн Леонід Михайлович
Каплун Валентина Аполінаріївна

Оригінал-макет підготовлено О. Войтович

Підписано до друку ……..
Формат 29,7×42¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різографічний. Ум. друк. арк. …...
Наклад … пр. Зам. № 2016-

Вінницький національний технічний університет,
навчально-методичний відділ ВНТУ.
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, к. 2201.
Тел. (0432) 59-87-36.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Віддруковано у Вінницькому національному технічному університеті
в комп'ютерному інформаційно-видавничому центрі.
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, ГНК, к. 114.
Тел. (0432) 59-85-32,
publish.vntu.edu.ua; email: kivc.vntu@gmail.com.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.