Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«05» 09 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ОСНОВИ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу моніторингу якості освіти
Протокол № 0128/22
(підпис) (прізвище, ініціали)
« » 2022 р.

2022 – 2023 навчальний рік

Розробники:

Коршун Наталія Володимирівна, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Коршун Наталія Володимирівна, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____ Павло СКЛАДАННИЙ
(підпис)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.
Керівник освітньої програми _____ Артем ПЛАТОНЕНКО
(підпис)

Робочу програму перевірено
___.___. 2022 р.
Заступник декана _____ Євген ІВАНІЧЕНКО
(підпис)

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»_____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	5 / 150	
Курс	3	
Семестр	5	
Кількість змістових модулів з розподілом:	4	
Обсяг кредитів	5	
Обсяг годин, в тому числі:	150	
Аудиторні	56	
Модульний контроль	8	
Семестровий контроль	30	
Самостійна робота	56	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Основи безпеки телекомунікаційних технологій» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека, освітньої програми 125.00.01 «Безпека інформаційних і комунікаційних систем».

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, які повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Основи безпеки телекомунікаційних технологій», та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Основи безпеки телекомунікаційних технологій» складається з чотирьох змістових модулів: Телекомунікаційні технології як об'єкти інформаційної безпеки; Багаторівневий захист інформації в телекомунікаційних мережах; Інструменти забезпечення інформаційної безпеки телекомунікаційних мереж; Забезпечення безпеки мережевої інфраструктури відповідно рівнів моделі OSI. Обсяг дисципліни – 150 год. (5 кредитів).

Метою викладання навчальної дисципліни «Основи безпеки телекомунікаційних технологій» є формування у студентів уміння вирішувати задачі забезпечення безпеки сучасних інформаційно-комунікаційних технологій, управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері інформаційної та кібернетичної безпеки та набутті **наступних компетентностей**:

Фахові компетентності:

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

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати:

- структури сучасних обчислювальних систем, методів і засобів обробки інформації, архітектури операційних систем;
- моделі управління мережевими ресурсами;
- програмні та апаратні засоби захисту в інформаційних системах;
- принципи побудови мережевих екранів;
- функції забезпечення безпеки мережевої інфраструктури відповідно рівнів еталонної моделі OSI;
- особливості реалізації статичних і динамічних VLAN;
- методику створення списків управління доступом (ACL);
- особливості управління багатоадресною розсилкою на 2-му рівні моделі OSI.

уміти:

- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
- застосовувати технології захисту інформації при міжмережевій взаємодії;
- виявляти мережеві атаки шляхом аналізу трафіка;
- застосовувати методи і засоби аналізу безпеки програмного забезпечення;
- застосовувати функції контролю підключення вузлів до портів комутатора;
- здійснювати планування захищеної мережі;
- застосовувати технології побудови віртуальних локальних мереж.

та досягти наступних ***програмних результатів навчання*:**

ПРз-2: здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних та SMART-технологій; розробляти та аналізувати проекти IT та SMART-систем базуючись на стандартизованих технологіях та протоколах передачі даних; здійснювати захист ресурсів і процесів в ІТС на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші), а також встановлених режимів безпечного функціонування IT та SMART-системах;

ПРз-3: забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

ПРз-4: вирішувати задачі супроводу (в тому числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в ІТС;

ПРз-9: забезпечувати неперервність бізнес процесів організації на базі системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісної і якісної оцінки.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Телекомунікаційні технології як об'єкти інформаційної безпеки							
Тема 1. Принципи побудови і функціонування телекомунікаційних мереж	12	4		4			4
Тема 2. Телекомунікаційні технології як об'єкти інформаційної безпеки	14	2			2		10
Модульний контроль	2						
Разом	28	6		4	2		14
Змістовий модуль 2. Багаторівневий захист інформації в телекомунікаційних мережах							
Тема 2. Багаторівневий захист інформації в телекомунікаційних мережах	28	6		4	4		14
Модульний контроль	2						
Разом	30	6		4	4		14
Змістовий модуль 3. Інструменти забезпечення інформаційної безпеки телекомунікаційних мереж							
Тема 3. Інструменти забезпечення інформаційної безпеки телекомунікаційних мереж	30	6		6	4		14
Модульний контроль	2						
Разом	32	6		6	4		14
Змістовий модуль 4. Забезпечення безпеки мережевої інфраструктури відповідно рівнів моделі OSI							
Тема 4. Забезпечення безпеки мережевої інфраструктури відповідно рівнів моделі OSI	28	6			8		14
Модульний контроль	2						
Разом	30	6			8		14
Підготовка та проходження контрольних заходів	30						
Усього	**150**	**24**		**14**	**18**		**56**

5. Програма навчальної дисципліни

Змістовий модуль 1. Телекомунікаційні технології як об'єкти інформаційної безпеки

Основні питання:

- Стратегії захисту інформації
- Принципи побудови і функціонування телекомунікаційних мереж
- Телекомунікаційні системи та технології як об'єкти інформаційної безпеки
- Основи безпеки інформаційних ресурсів
- Основи захвату та аналізу мережевого трафіку

Змістовий модуль 2. Багаторівневий захист інформації в телекомунікаційних мережах

Основні питання:

- Оцінка стану захисту мережі
- Протоколи стеку TCP/IP
- Актуальні загрози мережевій безпеці
- Захист інфраструктури мережі
- Захист технологій віддаленого доступу
- Захист інформації в корпоративних мережах
- Налагодження та дослідження роботи віртуальних локальних мереж
- Виявлення каналів несанкціонованого доступу до інформації
- Виявлення мережевих атак шляхом аналізу трафіку

Змістовий модуль 3. Інструменти забезпечення інформаційної безпеки телекомунікаційних мереж

Основні питання:

- Передача потоку даних. Багатоадресна розсилка
- Методи статичної та динамічної маршрутизації
- Методи маршрутизації за протоколами OSPF та EIGRP
- Налаштування статичної та динамічної маршрутизації за протоколом RIP

Змістовий модуль 4. Забезпечення безпеки мережевої інфраструктури відповідно рівнів моделі OSI

Основні питання:

- Забезпечення безпеки на канальному рівні моделі OSI
- Забезпечення безпеки на мережевому та транспортному рівнях моделі OSI
- Забезпечення безпеки на рівні додатків моделі OSI
- Налагодження та дослідження роботи списків керування доступом (Access Control List)
- Налагодження та дослідження засобів протидії атакам Port Security

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, залік.
- *Комп'ютерного контролю:* програми - емулятори.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;

- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	3	3	3	3	3	3	3	3
Відвідування практичних занять	1	2	2	2	2	3	3	-	-
Відвідування лабораторних занять	1	1	1	2	2	2	2	4	4
Робота на практичному занятті	10	2	20	2	20	3	30	-	-
Лабораторна робота (в тому числі допуск, виконання, захист)	10	1	10	2	20	2	20	4	40
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25	1	25
Виконання ІНДЗ	30								
Разом		-	66	-	77	-	88	-	77
Максимальна кількість балів: 308									
Розрахунок коефіцієнта: 308/60=5,13									

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Телекомунікаційні технології як об'єкти інформаційної безпеки		14	5
1	Об'єкти інформаційної безпеки. Безпека інформаційних ресурсів: ● виконання завдань відповідно до теми; ● опрацювання фахових видань.	14	5
Змістовий модуль 2. Багаторівневий захист інформації в телекомунікаційних мережах		14	5
2	Побудова захищених комп'ютерних мереж: ● виконання завдань відповідно до теми; ● опрацювання фахових видань.	14	5
Змістовий модуль 3. Інструменти забезпечення інформаційної безпеки телекомунікаційних мереж		14	5
3	Методи статичної та динамічної маршрутизації:	14	5

№ з/п	Назва теми	Кількість годин	Бали
	● виконання завдань відповідно до теми; ● опрацювання фахових видань.		
Змістовий модуль 4. Забезпечення безпеки мережевої інфраструктури відповідно рівнів моделі OSI		14	5
4	Мережева інфраструктура, відповідно рівнів моделі OSI: ● виконання завдань відповідно до теми; ● опрацювання фахових видань.	14	5
	Разом	56	20

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв’язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп’ютерний тест, що складається з 15 запитань закритої форми.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – комп’ютерний тест. Тест містить 20 тестових питань закритого типу (вибір правильної відповіді із запропонованих варіантів), які передбачають автоматичну (комп’ютерну) перевірку і оцінюються по 2 бали кожне. Екзамен оцінюється у 40 балів.

Орієнтовний перелік питань для семестрового контролю

1. Визначення та зміст стратегії.
2. Фактори внутрішнього і зовнішнього середовища, що впливають на необхідність захисту інформації.
3. Групи факторів, що впливають на захист інформації в інформаційних і комунікаційних системах.
4. Фактори, що впливають на захист інформації, які пов’язані з діяльністю людини.
5. Технологічні фактори та фактори рівня досягнень науково-технічного прогресу, що впливають на захист інформації.
6. Напрями забезпечення захисту інформації в інформаційних і комунікаційних системах.
7. Вимоги до стратегічних рішень.
8. Характеристика та зміст стратегій захисту інформації.
9. Задачі щодо забезпечення безпеки інформаційних технологій.

10. Принципи захисту інформації.
11. Основні принципи побудови системи забезпечення безпеки інформації.
12. Множина загроз інформації в інформаційно-комунікаційних системах (загрози порушення конфіденційності).
13. Множина загроз інформації в інформаційно-комунікаційних системах (загрози порушення цілісності).
14. Множина загроз інформації в інформаційно-комунікаційних системах (загрози порушення доступності чи відмовлення в обслуговуванні).
15. Множина загроз інформації в інформаційно-комунікаційних системах (загрози порушення спостережності чи керованості).
16. Джерела загроз безпеці інформації.
17. Класифікація середовищ виникнення джерел загроз.
18. Підмножини потоків інформаційно-телекомунікаційній системи, що пов'язані з несанкціонованим доступом.
19. Структура множини об'єктів доступу в інформаційно-телекомунікаційній системі.
20. Реалізація послідовності доступів до об'єктів в інформаційно-телекомунікаційній системі.
21. Правила реалізації доступу до об'єктів в інформаційно-телекомунікаційній системі.
22. Зміст множини асоційованих об'єктів.
23. Архітектурна безпека в корпоративних мережах.
24. Принципи архітектурної безпеки в корпоративних мережах.
25. Розмежування доступу клієнтів шляхом екранування.
26. Характеристика екранів як засобів розмежування доступу.
27. Характеристика екранів як послідовності фільтрів.
28. Типи захисту, що забезпечують мережеві екрани.
29. Характеристика екрануючих маршрутизаторів.
30. Класифікація мережевих екранів.
31. Характеристика транспортного екранування.
32. Характеристика екранів, що функціонують на прикладному рівні.
33. Багаторівневий захист корпоративних мереж.
34. Характеристика способів відправки пакетів від джерела до приймача в IP-мережах.
35. Адресація багатоадресної відправки пакетів в IP-мережах.
36. Характеристики множини асоційованих об'єктів.
37. Характеристики протоколу маршрутизації EIGRP.
38. Наведіть перелік основних часових параметрів протоколу EIGRP та їх значення за замовчуванням.
39. Які основні параметри повинні бути зазначені у таблиці маршрутизації маршрутизатора, що працює за протоколом EIGRP.
40. Наведіть основні команди налагодження протоколу EIGRP.
41. Характеристики протоколу маршрутизації OSPF.
42. Які основні параметри повинні бути зазначені у таблиці маршрутизації маршрутизатора, що працює за протоколом OSPF.
43. Наведіть перелік основних версій протоколу OSPF та зазначте їх відмінності.
44. Порядок налаштування функціонування протоколу маршрутизації RIP.
45. Команди діагностики настройок та роботи протоколу маршрутизації RIP.
46. Основні параметри маршрутизації маршрутизатора, що працює за протоколом RIP.
47. Методи статичної маршрутизації.
48. Переваги та недоліки використання статичної маршрутизації.
49. Маршрутизація за замовчуванням.
50. Способи спрощення налаштування статичної маршрутизації.
51. Команди налагодження маршрутизації між віртуальними локальними мережами.
52. Способи організації маршрутизації між віртуальними локальними мережами.
53. Забезпечення безпеки на транспортному рівні моделі OSI.
54. Керування сеансами TCP. Протокол UDP.

55. Варіанти застосування функції контролю підключення вузлів до портів комутатора.
56. Забезпечення безпеки на канальному рівні моделі OSI.
57. Механізми доступу до середовища та фреймування.
58. Забезпечення безпеки на рівні додатків моделі OSI.
59. Служби рівня додатків моделі OSI.
60. Забезпечення безпеки на мережному рівні моделі OSI.
61. Протоколи мережного рівня IPVN.
62. Маршрутизація на мережному рівні моделі OSI.
63. Особливості управління багатоадресною розсилкою на 2-му рівні моделі OSI (IGMP Snooping).
64. Планування захищеної мережі.
65. Організація захищеного підключення.
66. Особливості реалізації статичних і динамічних VLAN
67. Методика створення списків управління доступом (ACL).
68. Призначення і зміст списків управління доступом.
69. Типи профілів доступу.
70. Процес створення профілю доступу.
71. Приклади налаштування ACL.
72. Варіанти списків реалізації управління доступом (ACL).
73. Характеристика фізичного рівня еталонної моделі інформаційної мережі
74. Характеристика канального рівня еталонної моделі інформаційної мережі
75. Характеристика мережевого рівня еталонної моделі інформаційної мережі
76. Характеристика транспортного рівня еталонної моделі інформаційної мережі
77. Характеристика рівнів сеансів, представлення даних та прикладного еталонної моделі інформаційної мережі
78. Характеристика віддалених атак за умовою початку здійснення
79. Характеристика віддалених атак за наявністю зворотного зв'язку з об'єктом.
80. Характеристика віддалених атак за розташуванням суб'єкта атаки щодо об'єкта

Шкала відповідності оцінок

Рейтингова оцінка	**Сума балів за всі види навчальної діяльності**	**Значення оцінки**
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов’язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов’язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов’язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 150 год., лекції – 24 год., практичні заняття – 14 год., лабораторні роботи – 18 год., модульний контроль –8 год., самостійна робота –56 год., семестровий контроль – 30 год.

Модулі (назви, бали)	**Змістовий модуль 1. Телекомунікаційні технології як об'єкти інформаційної безпеки (66 балів)**			**Змістовий модуль 2. Багаторівневий захист інформації в телекомунікаційних мережах (77 балів)**			**Змістовий модуль 3. Інструменти забезпечення інформаційної безпеки телекомунікаційних мереж (88 балів)**			**Змістовий модуль 4. Забезпечення безпеки мережевої інфраструктури відповідно рівнів моделі OSI (77 балів)**		
Лекції (теми, бали)	№1 Загальні відомості про телекомунікаційні мережі і технології (1 бал)	№2 Еталонна модель взаємодії відкритих систем. Сімейство протоколів TCP/IP (1 бал)	№3 Телекомунікаційні технології як об'єкти інформаційної безпеки (1 бал)	№4 Оцінка стану захисту мережі (1 бал)	№5 Захист інфраструктури мережі (1 бал)	№6 Захист технологій віддаленого доступу (1 бал)	№7 Методика виявлення каналів несанкціонованого доступу до інформації (1 бал)	№8 Передача потоку даних. Багатоадресна розсилка (1 бал)	№9 Методи статичної та динамічної маршрутизації Протоколи OSPF та EIGRP (1 бал)	№10 Забезпечення безпеки на канальному рівні моделі OSI (1 бал)	№11 Забезпечення безпеки на мережевому та транспортному рівнях моделі OSI (1 бал)	№12 Забезпечення безпеки на рівнях додатків моделі OSI (1 бал)
Практичні, семінарські заняття (теми, бали)	№1 Пропускна здатність мереж в режимі комутації (11 балів)	№2 Вивчення моделі OSI (11 балів)		№3 Канали витоку інформації (11 балів)		№4 Конфігурація засобів захисту віддаленого доступу (11 балів)		№5-6 Протоколи динамічної маршрутизації (22 бали)	№7 Вивчення протоколу EIGRP (11 балів)			
Лабораторні заняття (теми, бали)			№1 Налаштування та дослідження роботи віртуальних локальних мереж (11 балів)	№2 Виявлення мережевих атак шляхом аналізу трафіку (11 балів)		№3 Виявлення мережевих атак шляхом аналізу трафіку (11 балів)		№4 Налагодження статичної та динамічної маршрутизації RIP (11 балів)	№5 Налагодження та дослідження роботи протоколу маршрутизації OSPF та EIGRP (11 балів)	№6 Побудова і налаштування VPN (11 балів)	№7-8 Налагодження та дослідження роботи списків керування доступом (Access Control List) (22 бали)	№9 Налагодження та дослідження засобів протидії атакам Port Security (11 балів)
Самостійна робота	Самостійна робота (5 балів)			Самостійна робота (5 балів)			Самостійна робота (5 балів)			Самостійна робота (5 балів)		
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)			Модульна контрольна робота 2 (25 балів)			Модульна контрольна робота 3 (25 балів)			Модульна контрольна робота 4 (25 балів)		
Підсумковий контроль (вид, бали)	Екзамен (40 балів)											

8. Рекомендовані джерела

Основні (базові):

1. Абрамов В.О. Комп'ютерні мережі: навчальний посібник. – К.: КУБГ, 2010. - 128 с.
2. Буров Є. В. Комп’ютерні мережі: підручник. - Львів: Магнолія 2006, 2018. - 260 с.
3. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П.М.. Технології забезпечення безпеки мережевої інфраструктури. - К.: КУБГ, 2019. – 218 с.
4. Бурячок В.Л., Гулак Г.М., Толубко В.Б.. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: підручник. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
5. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці. – К.:ДУТ, 2015. – 345 с.
6. Бурячок В.Л., Толюпа С.В., Семко В.В., Бурячок Л.В., Складанний П.М., Лукова-Чуйко Н.В.. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник. – К.: ДУТ - КНУ, 2016. – 178 с

Додаткові

1. Богуш В.М., Юдін О.К. Основи інформаційної безпеки держави. – К.: “МК-Прес”, 2005 – 432 с.
2. Богуш В.М., Кудін А.М. Інформаційна безпека від А до Я: 3000 термінів і понять. - К.: МОУ, 1999. - 456 с.
3. ДСТУ ISO/IEC 2382-17:2005. Інформаційні технології. Словник термінів. Частина 17. Бази даних.
4. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

9. Додаткові ресурси

1. History of LAN Switching. [електронний ресурс] http://www.myipaddressinfo.com
2. Evolution: 20 years of switching fabric. Ori Aruj, Dune Networks [електронний ресурс] http://www.commsdesign.com
3. On-chip Global Interconnects for Networking ASICs [електронний ресурс] http://www.lsi.com
4. Andreas D. Bovopoulos and Micha Zeiger. Shared-Memory Fabrics Meet 10-Gbit Backplane Demands. TeraChip, Inc. [електронний ресурс] http://www.commsdesign.com
5. Matching Output Queueing with a Combined Input Output Queued Switch [електронний ресурс] http://www-rcf.usc.edu
6. An improved algorithm for CIOQ switches. Yossi Azar, Ybssi Richter. [електронний ресурс] http://portal.acm.org
7. SciVerse ScienceDirect [електронний ресурс] http://www.sciencedirect.com
8. Institute of Electrical and Electronics Engineers http://www.ieee.org