Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки(№ 503)

ЗАТВЕРДЖУЮ

Голова НМК

Д .М. Крицький
(підпис) (ініціали та прізвище)

« 31 » сер пн я 2022 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Інформаційно-комунікаційні системи
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

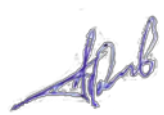
Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Форма навчання: денна

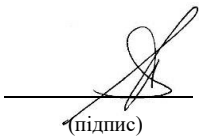
Рівень вищої освіти: перший (бакалаврський)

Харків 2022 рік

Розробник: Пєвнєв В.Я., доцент кафедри 503, к.т.н., доцент 
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 30 » 08 2022 р.

Завідувач кафедри д.т.н., професор  В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4</td><td rowspan="10">Галузь знань і
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність 125 "Кібербезпека"
(код та найменування)

Освітня програма
Безпека інформаційних комунікаційних систем
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 4</td><td>2022/2023</td></tr>
<tr><td>Індивідуальне завдання: РГР</td><td rowspan="2">Семестр: 5-й</td></tr>
<tr><td>Загальна кількість годин – 48/120</td></tr>
<tr><td rowspan="8">Кількість тижневих годин для денної форми навчання: аудиторних – 4 самостійної роботи студента – 7</td><td>Лекції *</td></tr>
<tr><td>24 години</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>24 години</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>72 годин</td></tr>
<tr><td>Індивідуальні завдання</td></tr>
<tr><td>6 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: Для денної форми навчання – 48/72.

* Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: вивчення можливостей та технологій сучасних інформаційно-комунікаційні мереж (ІКМ), основ їх побудови, супроводу і адміністрування.

Завдання: вивчення основних принципів побудови ІКМ; вивчення локальних ІКМ; вивчення мережевих архітектурних рішень; вивчення протоколів нижнього рівня ІКМ; вивчення питань проектування ІКМ; вивчення протоколів середнього і верхнього рівня ІКМ; вивчення способів адміністрування ІКМ.

Компетентності, які набуваються:

– здатність застосовувати знання у практичних ситуаціях;

– здатність та розуміння предметної області та розуміння професії;

– здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово;

– вміння виявити, ставити та вирішувати проблеми за професійним спрямуванням;

– здатність до пошуку, оброблення та аналізу інформації;

– здатність до використання інформаційно-комунікаційних технологій сучасних методів і моделей інформаційної безпеки та/або кібербезпеки;

– здатність до використання програмно та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних

– (автоматизованих) системах.

Очікувані результати навчання:

– застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

– організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

– використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

– аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

– готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки

– виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

– виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

– аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

– вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

– використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

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

– иирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

– 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).

– впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

– вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

– застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

– інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-

телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

– інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

– вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

Пререквізити – дисципліна базується на «Системи технічного захисту інформації», «Інформаційно-комунікаційні системи».

Кореквізити – «Дипломний робота (проект) бакалавра».

3. Програма навчальної дисципліни

Модуль 1

Змістовний модуль 1. ОС Cisco system, основи комутації, віртуальні локальні мережі, IP адресація та організація підмереж.

ТЕМА 1. Комутація мереж

Компоненти мережі. Представлення мереж. Діаграми топологій. Рівні та розподіл доступа.

ТЕМА 2. Операційні системи мережних пристроїв

Мережеві пристрої з операйійними системами. Система межмережної взаємодії Cisco. ***ТЕМА 3. Основи комутації.***

Процедура POST. Завнтаження ОС. Індикація стану комутатора.

Настроювання портів.

ТЕМА 4. Віртуальні локальні мережі

Визначення та переваги VLAN. Типи мереж. Транкові канали. Ідентифікація пакетів VLAN.

ТЕМА 5. Топології VLAN

Топології з надмірністю. Топології з резервуванням. Множинне перадавання фреймів. Бази MAC-адрес.

ТЕМА 6. Концепції маршрутизації.

Архітектура маршрутизаторів. Поєднання мереж. Вибір оптимального шляху. Пересилання пакетів. Шлюзи.

ТЕМА 7. IP адресація

Системи адрес та їх перетворення. Структура IP адреси. Типи адресації.

ТЕМА 8. Організація підмереж

Розподіл на підмережі, розрахунок та планування. Маски змінної дожини VLSM.

Модульний контроль. Модуль

Змістовний модуль 2. Статична і динамічна маршрутизація та протоколи маршрутизації, списки контроля доступу ACL, Перетворення мережних адрес та DHCP.

ТЕМА 9. Статична маршрутизація

Доступ до віддалених мереж. Переваги та доцільність статичної маршрутизації. Типи маршрутів. Команди роутера.

ТЕМА 10. Динамічна маршрутизація

Класифікація протоколів маршрутизації. Призначення протоколів динамічної маршрутизації. Обмін інформацією про мережі та маршрути.

Метрики протоколів.

ТЕМА 11. Маршрутизаці за станом каналу

Протоколи найкоротшого шляху. Протоколи за станом каналу. Алгоритм Дейкстри. Механізм Hello. Розсилка за станом каналу.

ТЕМА 12. Протокол OSPF.

Безкласовий протокол з підтримкою VLSM І CIDR. Суміжність пристроїв. Обмін маршрутною інформацією.

ТЕМА 13. Маршрутизація поміж VLAN.

Методи VLAN маршрутизації. Багаторівневий комутатор. Помилки в адресах та масках підмереж.

ТЕМА 14. Списки контроля доступу ACL.

Фільтрація пакетів. ACL списки. Wildcard маски. Робота з ACL списками.

ТЕМА 15. Перетворення мережних адрес.

Простір приватних IP адрес. Принципи та аналіз роботи NAT та PAT.

ТЕМА 16. Динамічна конфігурація вузлів DHCP.

Характеристика протоколу DHCP. Конфігурування та перевірка сервера. Автоматичне настроювання адреси та відслідковування її стану. Операції протоколу DHCPv6.

Модульний контроль.

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					

Змістовний модуль 1. ОС Cisco system, основи комутації, віртуальні локальні мережі, IP адресація та організація підмереж.					
Тема 1. Комутація мереж.	7	1	2		4
Тема 2. Операційні системи мережних пристроїв.	9	1	2		6
Тема 3. Основи комутації.	7	1			6
Тема 4. Віртуальні локальні мережі.	9	1	2		6
Тема 5. Топології VLAN.	10	2	2		6
Тема 6. Концепції маршрутизації.	8	2			6
Тема 7. IP адресація.	8	2	2		4
Тема 8. Організація підмереж.	10	2	2		6
Разом за змістовним модулем 1	68	12	12		44
Усього годин за модуль 1	68	12	12		44
Модуль 2					
Змістовний модуль 2. Статична і динамічна маршрутизація та протоколи маршрутизації, списки контроля доступу ACL, Перетворення мережних адрес та DHCP.					
Тема 1. Статична маршрутизація.	9	1	2		6
Тема 2. Динамічна маршрутизація.	9	1	2		6
Тема 3. Маршрутизаці за станом каналу.	3	1			2
Тема 4. Протокол OSPF.	3	1			2
Тема 5. Маршрутизація поміж VLAN.	8	2	2		4
Тема 6. Списки контроля доступу ACL.	10	2	2		6
Тема 7. Перетворення мережних адрес.	8	2	2		4
Тема 8. Динамічна конфігурація вузлів DHCP.	6	2	2		2
РГР	11				11
Разом за змістовним модулем 2	67	12	12		43
Усього годин за модуль 2	67	12	12		43
Усього годин за дисципліною	135	24	24		87

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин

...	*Не передбачено*	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Знайомство з CLI IoS. Базове налаштування комутатора.	2
2	Отримання практичних навичок з налаштування VLANs.	2
3	Отримання практичних навичок з розбиття на підмережі.	4
4	Отримання практичних навичок з статичної і динамічної маршрутизації.	4
5	Отримання практичних навичок з маршрутизації між віртуальними мережами.	4
6	Отримання практичних навичок з налаштування списків контролю доступу ACL.	4
7	Отримання практичних навичок з налаштування NAT/PAT.	4
	Разом	**24**

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	2	3
	Не передбачено	

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Загальне поняття протоколу. Еталонні моделі взаємодії комп'ютерних систем ISO/OSI та TCP/IP	10
2	Адресація в IP мережах	15
3	Маршрутизатори	15
4	Маршрутизація в IP-мережах	10
5	Безпека інформаційних і комунікаційних систем	10
6	Трансляція мережних адрес NAT/PAT	16
7	РГР	11
	Разом	**87**

9. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
1	РГР: Розробка комп'ютерної мережі і базове налаштування мережних пристроїв.	11

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
модуль 1			
Лекції	0…1	6	0…6
Практичні роботи	0...5	3	0…15
Модульний контроль	0…25	1	0..25
модуль 2			
Лекції	0…1	6	0…6
Практичні роботи	0…3	4	0…12
Модульний контроль	0…25	1	0…25
РГР	0…11	1	0…11
Усього за семестр			**0…100**

Контроль знань при проведенні занять оцінюється за такими шкалами: активність на лекції під час відповідей на питання:

- повна відповідь на питання - 1 бал;
- неповна відповідь – 0,5 балу; - відсутність на лекції - 0 балів, виконання і захист практичних робіт: при виконанні всіх вимог завдань методик на роботи - 4 бали;

- неповні відповіді на питання при захисті результатів роботи за змістом досліджуваної теми - 3 бали;
- неповні відповіді на питання за змістом і результатами роботи - 2 бала;
- недооформлені результати роботи і неповні відповіді на питання за змістом результатів роботи -1балл;
- якщо робота не виконана і не захищена - 0 балів.

На модульний контроль (всього 25 балів) виносяться всі пройдені за контрольований період теми, які включаються в варіанти завдань, що містять по 25 питанн (по всім темам та видам занять). Максимальна кількість балів за кожне питання - 1.

Семестровий контроль у вигляді іспиту проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних та одного практичного запитань, максимальна кількість за кожне із запитань, складає 33 балу.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 80% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняних та міжнародних стандартів для проведення наукових робіт та робіт щодо захисту інтелектуальної власності.

Добре (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 90% завдань практичних занять. Уміти використовувати сучасні методи теоретичних та експериментальних досліджень для організації та проведення наукових робіт. Мати необхідний обсяг вмінь для одержання позитивної оцінки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Уміти виконувати інформаційне забезпечення наукових досліджень.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

1. Презентації лекцій.
2. Керівництво до практичних робіт.

14. Рекомендована література. Базова

1. Комп'ютерні мережі. Принципи, технології, протоколи: Підручник для вузів/В. Г. Оліфер, Н. А. Оліфер - СПб.: Пітер, 2016. 864 с.
2. Локальні мережі: архітектура, алгоритми, проектування. / Новіков Ю. В., Кондратенко С.В. - М.: Еком, 2000. 312 с.
3. Таненбаум Еге. Комп'ютерні мережі. - СПб.: Пітер, 2014. 848 с.
4. Гук М. Апаратні засоби локальних мереж. Енциклопедія. - СПб.: Пітер, 2005. 576 с.

Допоміжна

1. Скотт Мюллер. Модернізація та ремонт ПК, 18-е видання. : Пров. з англ. – М.: ТОВ “І.Д. Вільямс”, 2009. 280 с.
2. Амато Віто. Основи організації мереж Cisco, том 1: Пер. з англ.- М.: Видав-нічий - будинок "Вільямс", 2002. 512 е.
3. Адміністрування мережі на прикладах. Поляк-Брагінський А. Ст – СПб.: БХВ-Петербург, 2005. 320 с.: іл.
4. Захист комп'ютерної інформації від несанкціонованого доступу. А. Ю. Щеглов. - СПб.: Видавництво "Наука і Техніка", 2004. 384 с.: Іл.
5. Основи інформаційної безпеки: курс лекцій: навчальний посібник
6. / Видання третє / Галатенко В.А. За ред. Академіка РАН В.Б. Бетеліна / - М.: ІН-ТУІТ.РУ «Інтернет-університет Інформаційних Технологій», 2006. 208 с.
7. Архітектура комп'ютерних систем та мереж: Навч. посібник/Т.П. Баранівська, В.І. Лойко та ін; за ред. В.І. Лойко. - М.: Фінанси та статистика, 2003. 256 с.: Іл.

15. Інформаційні ресурси

1. Архітектура комп'ютера [Електрон. ресурс]. - Режим доступу: http://inf1.info/book/export/html/44
2. Вікіпедія – вільна енциклопедія [Електрон. ресурс]. - Режим доступу: http://www. ru.wikipedia.org/
3. Вікіпедія - вільна енциклопедія [Електрон. ресурс]. – Режим доступу: http://www. ru.wikipedia.org/
4. Microsoft Virtual Academy [Електрон. ресурс]. - Режим доступу: http://www.microsoftvirtualacademy.com/
5. Microsoft IT Academy Program [Електрон. ресурс]. - Режим доступу: https://itacademy.microsoftelearning.com/
6. Cisco Networking Academy [Електрон. ресурс]. - Режим доступу: https://www.netacad.com/, http://www.cisco.com/web/learning/netacad/