Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут *електронних та інформаційних технологій*
Кафедра *кібербезпеки та математичного моделювання*

СИЛАБУС
Управління мережевою безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ткач Ю.М._____
(підпис) (прізвище та ініціали)

« 26 » серпня 2024 р.

Розробник: Семендяй Сергій Матвійович, старший викладач кафедри кібербезпеки та математичного моделювання _____
Гребенник Алла Григорівна, старший викладач кафедри кібербезпеки та математичного моделювання _____

(підпис)

Силабус навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від « 26 » серпня 2024 р. № 7

Узгоджено з гарантом освітньої програми: _____ Ткач Ю.М.
(підпис) (прізвище та ініціали)

1. Загальна інформація про дисципліну

Тип дисципліни	*Обов'язкова*
Мова викладання	українська
Рік навчання та семестр	1 рік, 1 семестр 125 «Кібербезпека та захист інформації» ОПП «Кібербезпека»
Викладач (-і)	Семендяй Сергій Матвійович, старший викладач кафедри кібербезпеки та математичного моделювання Гребенник Алла Григорівна, старший викладач кафедри кібербезпеки та математичного моделювання
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/ https://scholar.google.com/citations?hl=ru&user=0T31xGYAAAAJ

	https://orcid.org/0000-0002-7751-5956 https://www.scopus.com/authid/detail.uri?authorId=58751294500 https://mmi.stu.cn.ua/personal-kafedry/ https://scholar.google.fi/citations?hl=uk&user=zDx8WrsAAAAJ https://www.scopus.com/authid/detail.uri?authorId=57219054928 https://orcid.org/0000-0002-7464-1412
Контакти викладача	+380952859046, serhii_semendiai@icloud.com контактний телефон: +380977267613, E-mail: grebennik.alla@gmail.com

2. Анотація курсу

Дисципліна «Управління мережевою безпекою» є складовою частиною програми підготовки магістрів ОПП «Кібербезпека» за спеціальністю 125 «Кібербезпека та захист інформації», галузь знань 12 «Інформаційні технології».

Управління мережевою безпекою є актуальною, технічною, теоретичною та практичною проблемою забезпечення конфіденційності, цілісності та доступності інформації в різних областях застосування інформаційно-комунікаційних мереж – в сфері зв'язку, військовій справі й системах безпеки країни, корпоративних інформаційних системах, системах моніторингу та управління, повсякденній діяльності людини. Для забезпечення безпечного функціонування сучасних інформаційних систем необхідно надійне і ефективне управління не тільки самими мережами, але і засобами мережевої безпеки. Висококваліфіковані фахівці в сфері кібербезпеки повинні вміти захистити інформаційні ресурси мережі від найбільш поширених зовнішніх і внутрішніх атак, спрямованих на виведення з ладу серверів і знищення даних, від небажаного проникнення в локальні обчислювальні мережі через «діри» в ОС, від цілеспрямованого вторгнення в систему через інформаційно-комунікаційні мережі для отримання конфіденційної інформації тощо.

Підхід до викладання спрямований на розширення кола застосування набутих раніше знань та практичних навичок для вирішення практичних завдань в майбутній професійній діяльності, до яких традиційно включають і задачі управління мережевою безпекою та організації захисту інформаційно-комунікаційних систем. Оволодіння програмою курсу сприяє виконанню студентами завдань з інших дисциплін, які передбачають наукові та практичні (інженерні) дослідження в напрямку безпеки інформаційно-комунікаційних мереж, узагальнення теоретичного матеріалу і поглиблення практичних навичок в сфері управління мережевою безпекою. Окрім цього, засвоєння дисципліни дозволить майбутнім фахівцям забезпечити необхідний рівень володіння інструментами управління, проектування і захисту мереж, що дасть можливість більш глибокого розуміння особливостей захисту інформації в інформаційно-комунікаційних мережах.

Посилання на курс в MOODLE: https://eln.stu.cn.ua/course/view.php?id=4370

3. Мета та цілі курсу

Метою викладання дисципліни є формування у здобувачів вищої освіти (ЗВО) комплексу знань щодо основ менеджменту інформаційної безпеки, набуття теоретичних знань та практичних навичок щодо управління інформаційною безпекою в інформаційно-телекомунікаційних системах для реалізації встановленої політики безпеки, формування науково-професійного світогляду магістра спеціальності 125 «Кібербезпека та захист інформації» в області використання цих технологій для захисту інформації під час її передачі інформаційно-комунікаційними мережами та в повсякденній професійній діяльності; розкриття сучасних методів захисту інформації в комп'ютерних мережах і ознайомлення з особливостями їх апаратної та програмної реалізацій.

Під час вивчення дисципліни ЗВО має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності 125 «Кібербезпека та захист інформації»:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 3. Здатність до абстрактного мислення, аналізу та синтезу.

КФ 1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ 4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ 5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ 6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ 9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

4. Результати навчання

За результатами вивчення курсу студенти повинні:

Знати:

- основні поняття, принципи та моделі управління мережею і мережевою безпекою;
- загрози інформаційній безпеці в обчислювальних та корпоративних мережах;
- стандарти і нормативні документи у сфері мережевої безпеки (ISO/IEC, NIST, НД ТЗІ тощо);
- архітектуру та функціональні можливості міжмережевих екранів, IDS/IPS, VPN;
- принципи побудови захищених віртуальних мереж (VPN) і механізми криптографічного захисту;
- протоколи автентифікації та управління доступом (RADIUS, TACACS+, Kerberos, LDAP, SNMP);
- методи та засоби моніторингу і аудиту безпеки мереж;
- сучасні тенденції розвитку безпекових мережевих технологій та їхні обмеження.

Вміти:

- аналізувати архітектуру корпоративної мережі та визначати її вразливості;
- розробляти політику безпеки для корпоративної мережі та реалізовувати її за допомогою технічних і адміністративних засобів;
- налаштовувати міжмережеві екрани, VPN, IDS/IPS та інші засоби захисту;
- застосовувати протоколи автентифікації та управління доступом у практичних завданнях;
- проводити аудит, моніторинг і тестування мережевої безпеки;
- впроваджувати сегментацію мереж і принципи мінімальних привілеїв;
- оцінювати ефективність систем захисту з використанням критеріїв продуктивності, надійності й відповідності стандартам;
- використовувати спеціалізоване програмне та апаратне забезпечення для виявлення й протидії мережевим атакам.

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових

результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

5. Пререквізити

Дисципліна є складовою частиною Обов'язкових дисциплін циклу професійної підготовки. Вивчення курсу передбачає наявність систематичних та ґрунтовних знань.

6. Обсяг курсу.

Вид заняття	Загальна кількість годин (очна/заочна форма навчання)
Лекції	16/6
Лабораторні заняття	16/6
Самостійна робота	88/108
Індивідуальне завдання: *розрахунково-графічна робота*	

Всього кредитів – *4*	120

7. Тематика курсу

Змістовий модуль 1. Теоретичні основи управління мережевою безпекою

Тема 1. Основні поняття та базові принципи управління мережевою безпекою – 1 година

Предмет та завдання курсу “Управляння мережевою безпекою”. Централізоване та розподілене управління мережею. Проблеми що виникають при створенні комп’ютерних мереж і систем. Особливості інформації, що передається в системах. Основні джерела інформації: стандарти ICTT/ITU, рекомендовані стандарти RFC, а також документація до програмних пакетів що вивчаються. Допоміжні джерела інформації в мережі Інтернет. Огляд методів та засобів захисту комп'ютерних мереж. Методи проведення атак. Апаратні, програмні та програмно-апаратні засоби захисту.

Тема 2. Проблеми інформаційної безпеки мереж – 1 година

Мережевий інформаційний обмін. Аналіз загроз мережевої безпеки. Модель комп`ютерної мережі. Модель загроз безпеки. Модель протидії загрозам безпеки. Забезпечення інформаційної безпеки мереж. Основні поняття політики безпеки. Структура політики безпеки організації.

Тема 3. Методи та засоби забезпечення мережевої безпеки – 2 години

Тенденції розвитку безпекових мережевих технологій. Засади організації захисту інформації в корпоративних мережах. Принципи надання доступу до IP в корпоративних мережах. Застосування систем виявлення вторгнень до корпоративних мереж. Структуризація сучасних систем виявлення вторгнень. Класифікація політик виявлення вторгнень. Практика застосування політики IDS.

Тема 4. Управління мережевою безпекою на основі стеку протоколів – 2 години

Стандартні стеки комунікаційних протоколів. Модель і стек протоколів OSI. Стек протоколів TCP/IP. Проблеми безпеки IP-мереж. IP версія 4. IP версія 6. Безпека на фізичному рівні. Безпека на канальному рівні. Безпека на мережевому рівні. Безпека на транспортному рівні. Безпека на сеансовому рівні. Інфраструктура захисту на прикладному рівні.

Тема 5. Методи управління засобами мережевої безпеки – 1 година

Завдання управління системою мережевої безпеки. Архітектура управління засобами мережевої безпеки. Функціонування системи управління засобами безпеки. Аудит і моніторинг безпеки.

Тема 6. Проблеми безпеки під час використання Інтернет – 1 година

Електронний бізнес і проблеми безпеки. Основні моделі електронної комерції. Здійснення електронних платежів через Інтернет. Інтернет-банкінг, трейдинг та страхування. Потенційні загрози для електронного бізнесу. Шляхи розв`язання проблем безпеки електронного бізнесу.

Змістовий модуль 2. Прикладні аспекти управління мережевою безпекою

Тема 7. Інструменти забезпечення мережевої безпеки сучасних операційних систем – 2 години

Проблеми забезпечення мережевої безпеки ОС. Загрози безпеки ОС. Поняття захищеної ОС. Адміністративні заходи захисту. Архітектура підсистеми захисту ОС. Основні функції підсистеми захисту ОС. Ідентифікація, аутентифікація і авторизація суб'єктів доступу. Розмежування доступу до об'єктів ОС. Аудит.

Тема 8. Управління безпекою бездротових мереж – 2 години

Особливості організації бездротових мереж. Вразливості бездротових мереж. Кібератаки на бездротові мережі. Захист бездротових мереж.

Тема 9. Особливості міжмережевого екранування – 1 година

Екрануючий маршрутизатор. Шлюз сеансового рівня. Прикладний шлюз. Встановлення і конфігурування систем FireWall. Розробка політики міжмережевої взаємодії. Визначення схеми підключення міжмережевого екрану. Налаштування параметрів функціонування брандмауера. Критерії оцінки міжмережевих екранів. Сучасні системи FireWall. Переваги і недоліки. Підтримка різних платформ і режимів роботи. Ефективність управління. Підтримка функцій захисту. Сигналізація і реєстрація. FireWall-1. Gauntlet. BlackHole.

Тема 10. Побудова захищених віртуальних мереж VPN – 1 година

Концепція побудови віртуальних захищених мереж VPN. VPN рішення для побудови захищених мереж. Переваги застосування технологій VPN. Побудова захищених віртуальних мереж на базі маршрутизаторів. Побудова захищених віртуальних мереж за допомогою міжмережевих екранів. Побудова захищених віртуальних мереж на основі спеціалізованого програмного забезпечення. Побудова захищених віртуальних мереж на основі спеціалізованих апаратних засобів.

Тема 11. Безпека віддаленого доступу до комп'ютерної мережі – 1 година

Аутентифікація віддалених користувачів. Протокол PAP. Протокол S/Key. Протокол CHAP. Протидія несанкціонованому міжмережевому доступу. Фільтрація трафіку. Виконання функцій посередництва. Централізований контроль віддаленого доступу. Сервери віддаленого доступу.

Тема 12. Мережеві протоколи ідентифікації та автентифікації – 1 година

Мережеві протоколи автентифікації та управління. Системи AAA. Налагодження серверу AAA. Мережевий протокол SNMP. Системи виявлення та протидії мережевим атакам. Налаштування мережевого обладнання рівня доступу та ядра мережі. Системи захисту обчислювальних мереж. Системи виявлення порушника.

8. Система оцінювання та вимоги

Загальна система оцінювання курсу	Оцінювання курсу базується на накопичувальній системі та включає: поточний контроль (оцінювання лабораторних занять) – 42 бали, проміжний модульний контроль – 8 балів, виконання індивідуального завдання (РГР) – 10 балів та підсумковий контроль – 40 балів. Оцінювання кожного виду діяльності здійснюється окремо відповідно до досягнення навчальних цілей.
Вимоги до РГР	Критерії оцінювання РГР: 1) виконання завдання – 5 балів; 2) якість виконання завдання – 2 бали; 4) оформлення роботи, відповідність методичним рекомендаціям – 2 бали; 5) своєчасність здачі роботи – 1 бал.
Лабораторні заняття	Оцінка кожного лабораторного заняття здійснюється за наступними критеріями: 1) виконання практичного завдання – 4 бали; 2) аналіз отриманих результатів – 2 бали; 3) належне оформлення звіту – 1 бал.
Умови допуску до підсумкового контролю	1. Виконання та захист усіх лабораторних робіт. 2. Проходження проміжного модульного контролю. 3. Виконання розрахунково-графічної роботи.

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю	**Кількість балів**

Змістовий модуль 1. Теоретичні основи управління мережевою безпекою		**0...25/25**
1	Виконання лабораторних робіт	**0…21/21**
2	Проміжний модульний контроль	**0…4/4**
Змістовий модуль 2. Прикладні аспекти управління мережевою безпекою		**0...25/25**
1	Виконання лабораторних робіт	**0…21/21**
2	Проміжний модульний контроль	**0…4/4**
Усього поточний і проміжний модульний контроль		**0...50/50**
Виконання індивідуального завдання (РГР)		**0...10/10**
Семестровий контроль (Екзамен)		**0...40/40**
Разом		**0…100/100**

Шкала оцінювання результатів навчання

Оцінка в балах	**Оцінка ECTS**	**Оцінка за національною шкалою (диференційований залік)**	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		
0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

9. Обладнання та програмне забезпечення

При вивченні цього курсу для дистанційного навчання, тестування та обговорення питань курсу використовуються платформи *Moodle* та *Microsoft Teams*, для виконання лабораторних робіт застосовується комутаційне й серверне обладнання, а також ПК та програмне забезпечення навчальних аудиторій 105, 106, 110, 111 кафедри кібербезпеки та математичного моделювання.

10. Політики курсу

У випадку, якщо здобувач протягом семестру не виконав у повному обсязі всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (25), він не допускається до складання екзамену під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань здобувачів НУ “Чернігівська політехніка”». Повторне складання екзамену з метою підвищення позитивної оцінки не дозволяється. У випадку повторного складання екзамену всі набрані протягом семестру бали анулюються, а повторний екзамен складається у вигляді тестування.

До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до «Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка»». Запорукою успішного вивчення дисципліни є активність та залучення під час проведення лабораторних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних задач. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій (через вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».

Політика дедлайнів

Своєчасність здачі лабораторної роботи оцінюється в 0,5 балу за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 1 бал. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом тощо).

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 10 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу, зокрема при виконанні лабораторних та розрахунково-графічних робіт (принципи описані у Кодексі академічної доброчесності НУ «Чернігівська політехніка»). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

11. Рекомендована література

Базова

1. Микитишин А. Г., Митник М. М., Голотенко О. С., Карташов В. В. Комплексна безпека інформаційних мережевих систем: навч. посіб. – Тернопіль: ФОП Паляниця В. А., 2023. – 324 с.

2. Комп'ютерні мережі: контроль та прогнозування перевантажень. Навчальний посібник/ О.М. Ткаченко, Я.І. Торошанко, А.В. Лемешко, В.О. Сосновий, С.С. Коротков., К. : ДУТ, 2021, 77с.

3. Захист інформації в комп'ютерних системах : підруч. для студ. спец. 123 «комп'ютерна інженерія» / уклад. : О. М. Гапак, С. І. Балога ; рец. : М. І. Глебена. – Ужгород : ПП "АУТДОР-ШАРК, 2021. – 184 с.

4. Cardwell K. Tactical Wireshark. Berkeley, CA : Apress, 2023. URL: https://doi.org/10.1007/978-1-4842-9291-4 (дата звернення: 07.08.2024).

5. Haddadou K., Pujolle G. Cloud and Edge Networking. – Newark : John Wiley & Sons, Incorporated, 2024. – 303 с. – ISBN 978-1-78945-128-3.

Допоміжна

1 Лемешко А.В. Проектування безпроводових комп'ютерних мереж: навч. посібник / А.В. Лемешко, Л.А. Кирпач, Д.В. Сорокін, І.А. Бученко, М.М. Шрам. — К. : ДУТ, 2021. — 147 с.

Інформаційні ресурси

1. Система дистанційного навчання НУ «Чернігівська політехніка». Курс: Управління мережевою безпекою (ОК9). e-Learning НУ "Чернігівська політехніка". URL: https://eln.stu.cn.ua/course/view.php?id=4370 (дата звернення: 07.08.2024).

2. RouterOS. MikroTik Documentation. MikroTik Routers and Wireless - Support. URL: https://help.mikrotik.com/docs/spaces/ROS/pages/328059/RouterOS (дата звернення: 07.08.2024).

3. Cisco Networking Academy: Learn Cybersecurity, Python & More. Cisco Networking Academy: Learn Cybersecurity, Python & More. URL: https://www.netacad.com (дата звернення: 07.08.2024).

4. Електронний архів Національного університету «Чернігівська політехніка». Головна сторінка IRChNUT. URL: https://ir.stu.cn.ua/?locale-attribute=uk (дата звернення: 07.08.2024).

5. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua (дата звернення: 07.08.2024).

6. Законодавство України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws (дата звернення: 07.08.2024).