МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету
_____ Інна КОНДЮС
«29» серпня 2026 р.

ЗАТВЕРДЖУЮ
Перший проректор
_____ Надія КОВАЛЬЧУК
«29» серпня 2026 р.

СИЛАБУС

з освітнього компонента «Мережеві технології і протоколи»
ступінь вищої освіти – бакалавр
галузь знань – F Інформаційні технології
спеціальність – F5 Кібербезпека та захист інформації
освітня програма – Кібербезпека

Кафедра кібербезпеки

Силабус склав(ла) доцент кафедри кібербезпеки, к.т.н., доцент Сергій ГРИНЮК

Силабус затверджений на засіданні кафедри кібербезпеки, протокол № 2 від «28» серпня 2026 р.

Завідувач кафедри к.т.н., доцент Сергій КОСТЮЧКО

Розглянуто та схвалено групою забезпечення освітньої програми «Кібербезпека», протокол № 2 від «28» серпня 2026 р.

Гарант ОП «Кібербезпека» к.т.н., доцент Сергій КОСТЮЧКО

Схвалено науково-методичною радою університету, протокол № 1/а від «29» серпня 2026 р.

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/205

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Мережеві технології і протоколи»

Освітня програма	Кібербезпека
Галузь знань / Спеціальність	F Інформаційні технології / F5 Кібербезпека та захист інформації
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	нормативна
Мова викладання	українська
Обсяг	6 кредитів ECTS / 180 годин, семестр 3
Форма контролю	екзамен
Викладач(і)	к.т.н., доцент Сергій ГРИНЮК електронна пошта: sgrunjuk@lutsk-ntu.com.ua

1. Мета і завдання дисципліни

Мета: Метою викладання навчальної дисципліни «Мережеві технології і протоколи» є формування у здобувачів вищої освіти системи теоретичних знань і практичних навичок щодо принципів побудови та функціонування комп'ютерних мереж, призначення, структури й механізмів роботи протоколів усіх рівнів мережевої взаємодії, а також здатності аналізувати захищеність протоколів і обґрунтовано обирати засоби їх захисту відповідно до вимог інформаційної та кібербезпеки.

Завдання: - вивчення принципів багаторівневої організації мереж на основі еталонної моделі OSI та стека протоколів TCP/IP;
– опанування протоколів канального рівня та технологій комутації: Ethernet, STP/RSTP, 802.1Q, LACP;
– вивчення протоколів мережевого рівня (IPv4, IPv6, ARP, ICMP) і принципів адресації та трансляції адрес;
– опанування протоколів маршрутизації та розуміння механізмів їх захисту;
– вивчення протоколів транспортного рівня (TCP, UDP, QUIC) і механізмів забезпечення надійності передавання;
– опанування протоколів мережевих служб і прикладного рівня: DNS, DHCP, NTP, HTTP, SMTP, FTP, MQTT;
– вивчення криптографічних протоколів захищеного передавання даних (TLS, IPsec, WireGuard, SSH);
– опанування протоколів керування та моніторингу мережі (SNMP, syslog, NetFlow, NETCONF);
– формування навичок аналізу протоколів засобами захоплення трафіку та виявлення відхилень від специфікації;
– ознайомлення з класифікацією атак на мережеві протоколи та сучасними тенденціями їх розвитку.

Пререквізити: Фізика, Основи кібербезпеки

2. Компетентності

ІК — інтегральна компетентність: Здатність розв’язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

ЗК08 — Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

СК02 — Здатність використовувати інформаційні технології, сучасні методи і моделі

кібербезпеки та системи захисту інформації.

3. Структура дисципліни, розподіл годин, зв'язок тем з компетентностями

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
Змістовий модуль 1. Мережеві технології та протоколи базових рівнів								
1	Тема 1. Вступ до дисципліни. Мережеві технології та протоколи в системі забезпечення кібербезпеки	2/0,5	2/0,5	7/10	11/11	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	ЗК08, СК02
2	Тема 2. Еталонна модель OSI та стек протоколів TCP/IP. Інкапсуляція даних	2/0,5	2/0,5	7/10	11/11	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
3	Тема 3. Протоколи фізичного та канального рівнів. Технології Ethernet і комутація	2/0,5	2/0,5	7/10	11/11	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
4	Тема 4. Протоколи віртуальних локальних мереж та агрегації каналів	2/0,5	2/0,5	7/10	11/11	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
5	Тема 5. Протоколи мережевого рівня: IPv4, ARP, ICMP. Адресація та трансляція адрес	2/0,5	2/0,5	7/10	11/11	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
6	Тема 6. Протокол IPv6	2/0,5	2/0,5	7/10	11/11	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
7	Тема 7. Протоколи маршрутизації	2/0,5	2/0,5	7/10	11/11	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
8	Тема 8. Протоколи транспортного рівня: TCP, UDP, QUIC	2/0,5	2/0,5	7/9,75	11/10,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
Змістовий модуль 2. Протоколи прикладного рівня, керування та захисту								

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
9	Тема 9. Протоколи мережевих служб: DNS, DHCP, NTP	2/0,5	2/0,5	7/9,75	11/10,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	ЗК08, СК02
10	Тема 10. Протоколи веб-служб та обміну даними між застосунками	2/0,25	2/0,25	7/9,75	11/10,25	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
11	Тема 11. Протоколи електронної пошти та передавання файлів	2/0,25	2/0,25	6/9,75	10/10,25	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
12	Тема 12. Протоколи бездротових мереж та Інтернету речей	2/0,25	2/0,25	6/9,75	10/10,25	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
13	Тема 13. Криптографічні протоколи захищеного передавання даних	2/0,25	2/0,25	6/9,75	10/10,25	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
14	Тема 14. Протоколи керування та моніторингу мережі	2/0,25	2/0,25	6/9,75	10/10,25	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
15	Тема 15. Аналіз мережевих протоколів для потреб кібербезпеки. Сучасні тенденції	2/0,25	2/0,25	6/9,75	10/10,25	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, захист лабораторної роботи	СК02
	ІЗ/КПІЗ			20/20	20/20			
	Разом	**30/6**	**30/6**	**120/168**	**180/180**			

Легенда: ЗК — загальна компетентність (номер за п. 2); СК — спеціальна (фахова) компетентність (номер за п. 2). Повне формулювання кожного коду наводиться в ОП / стандарті спеціальності.

Методи навчання: МН1 — словесний метод (лекція, дискусія, співбесіда тощо); МН2 — практичний метод (лабораторні та практичні заняття); МН3 — наочний метод (метод ілюстрацій і метод демонстрацій); МН4 — робота з навчально-методичною літературою (конспектування, тезування, анотування, рецензування, складання реферату); МН5 — відеометод у сполученні з новітніми інформаційними технологіями та комп'ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані тощо).

Методи оцінювання: МО1 — екзамен; МО2 — усне або письмове опитування; МО4 — тестування.

4. Результати навчання

ПРН03. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів

недоброчесності у професійній діяльності.

ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

ПРН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й Інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.

5. Цілі сталого розвитку

ЦСР 4 – Якісна освіта

ЦСР 9 – Промисловість, інновації та інфраструктура

6. Неформальна освіта

Рекомендовані курси, тренінги, стажування та інші: результати навчання, здобуті у формальній, неформальній чи інформальній освіті, можуть бути визнані відповідно до процедур ЛНТУ. Підтвердженнями можуть бути сертифікати тематичних тренінгів, вебінарів чи онлайн-курсів разом з описом досягнутих результатів навчання та, за потреби, коротке верифікаційне завдання або портфоліо.

7. Критерії та форми контролю

Оцінювання — за 100-бальною шкалою (національна шкала / ЄКТС). Підсумковий бал = поточний контроль (30 %) + ІЗ/КПІЗ (10 %) + модульний контроль (20 %) + екзамен (40 %).

Академічна доброчесність: самостійне виконання завдань; коректне посилання на джерела; позначення частин тексту, згенерованих засобами ШІ. Порушення академічної доброчесності не толеруються.

8. Зміст тем

Тема 1. Вступ до дисципліни. Мережеві технології та протоколи в системі забезпечення кібербезпеки

Роль мережевих технологій і протоколів у професійній діяльності фахівця з кібербезпеки. Поняття протоколу та його складники: синтаксис, семантика, часові співвідношення. Стек протоколів, інтерфейс і служба. Основні поняття: вузол, канал, середовище передавання, адреса. Класифікація мереж за масштабом (PAN, LAN, CAN, MAN, WAN) та способом комутації. Фізичні й логічні топології. Клієнт-серверна, однорангова та багаторівнева архітектури. Організації зі стандартизації: ISO, ITU-T, IEEE, IETF, IANA, ДСТУ; статуси документів RFC та порядок роботи з ними. Показники якості функціонування мережі: пропускна здатність, затримка, джитер, втрати пакетів, доступність. Протокол як об'єкт атаки: розбіжність між специфікацією та реалізацією як джерело вразливостей.

Тема 2. Еталонна модель OSI та стек протоколів TCP/IP. Інкапсуляція даних

Принцип багаторівневої організації мережевої взаємодії. Сім рівнів моделі OSI: функції та типові протоколи кожного рівня. Стек TCP/IP і його відповідність моделі OSI. Протокольні блоки даних (PDU). Процеси інкапсуляції та деінкапсуляції. Поля демультиплексування: EtherType, Protocol, номер порту. Наскрізна та покрокова взаємодія; які заголовки змінюються під час проходження через проміжні пристрої. Порядок байтів і подання полів у заголовках протоколів. Загрози, характерні для окремих рівнів моделі, як основа побудови ешелонованого захисту.

Тема 3. Протоколи фізичного та канального рівнів. Технології Ethernet і комутація

Характеристики середовищ передавання: мідні кабелі (UTP/FTP/STP, категорії 5e–8), волоконно-оптичні кабелі, безпровідні середовища. Стандарти TIA/EIA-568, ISO/IEC 11801. Методи лінійного кодування: NRZ, NRZI, Manchester, 4B/5B, 8B/10B, PAM. Підрівні LLC (IEEE 802.2) і MAC. Стандарти IEEE 802.3, формат кадру Ethernet II, MAC-адресація. Принцип роботи комутатора, таблиця MAC-адрес, домени колізій і широкомовні домени. Протоколи STP, RSTP,

MSTP: ідентифікатор моста, ролі та стани портів, час збіжності. Виявлення помилок за алгоритмом CRC-32. Атаки канального рівня: MAC-flooding, MAC-spoofing, маніпуляції BPDU; засоби протидії

Тема 4. Протоколи віртуальних локальних мереж та агрегації каналів

Призначення VLAN: сегментація широкомовних доменів, ізоляція потоків трафіку, підвищення керованості й безпеки. Типи VLAN: даних, голосова, керування, native. Протокол тегування IEEE 802.1Q: структура тега, пріоритет 802.1p. Транкові порти, протокол DTP і ризики його використання. Міжмережева взаємодія VLAN: router-on-a-stick, комутатор третього рівня, SVI. Протокол агрегації каналів LACP (IEEE 802.3ad) та статичне об'єднання портів. Приватні VLAN і мікросегментація. Атаки VLAN hopping (switch spoofing, double tagging) та засоби протидії.

Тема 5. Протоколи мережевого рівня: IPv4, ARP, ICMP. Адресація та трансляція адрес

Функції мережевого рівня, структура заголовка IPv4 та призначення кожного поля. Класова та безкласова (CIDR) адресація, маска підмережі, префікс. Публічні та приватні адреси (RFC 1918). Планування адресного простору: підмережі фіксованої довжини та VLSM. Фрагментація та збирання дейтаграм. Протокол ARP: формат повідомлень, кеш, безадресний (gratuitous) ARP, атака ARP-spoofing. Протокол ICMP: типи й коди повідомлень, застосування в утилітах ping і traceroute, зловживання (ICMP-тунелювання, розвідка). Трансляція адрес NAT/PAT: види, переваги та обмеження з погляду безпеки й аналізу трафіку.

Тема 6. Протокол IPv6

Передумови переходу до IPv6. Структура основного заголовка та заголовки розширення. Формати запису та типи адрес: глобальні unicast, link-local, unique local, multicast, anycast. Ідентифікатор інтерфейсу, EUI-64, тимчасові адреси. Протокол ICMPv6 та його роль. Протокол виявлення сусідів ND: повідомлення RS, RA, NS, NA. Автоконфігурація SLAAC та протокол DHCPv6 (stateless і stateful). Механізми співіснування з IPv4: dual-stack, тунелювання, трансляція. Специфічні загрози: rogue RA, RA-flooding, зловживання ND; засоби протидії (RA Guard, ND Inspection).

Тема 7. Протоколи маршрутизації

Функції маршрутизатора, структура таблиці маршрутизації, принцип найдовшого збігу префікса. Адміністративна відстань і метрика. Статичні маршрути: звичайні, підсумовуючі, за замовчуванням, плаваючі. Класифікація протоколів динамічної маршрутизації: дистанційно-векторні та за станом каналу; внутрішньодоменні (IGP) і міждоменні (EGP). Протоколи RIPv2 і RIPng. Протокол OSPF: типи пакетів, установлення сусідства, база даних стану каналів, повідомлення LSA, алгоритм SPF, зони, типи маршрутизаторів. Протокол EIGRP: алгоритм DUAL, метрика, таблиці. Автономні системи та протокол BGP: типи сесій, атрибути шляху, політики. Загрози маршрутизації: підміна оновлень, BGP hijacking, route leaks; автентифікація оновлень, фільтрація маршрутів, механізми RPKI.

Тема 8. Протоколи транспортного рівня: TCP, UDP, QUIC

Функції транспортного рівня: сегментація, мультиплексування, адресація застосунків. Порти та сокети, категорії номерів портів. Протокол UDP: формат дейтаграми, сфери застосування, контрольна сума. Протокол TCP: структура заголовка, прапорці, установлення з'єднання, нумерація й підтвердження, повторне передавання, завершення сеансу. Керування потоком (ковзне вікно) та керування перевантаженням (Reno, Cubic, BBR). Протокол QUIC і транспорт HTTP/3: об'єднання транспортних і криптографічних функцій. Механізми забезпечення якості обслуговування. Атаки на транспортний рівень: SYN-flood, сканування портів, перехоплення сеансу; протидія (SYN cookies, обмеження інтенсивності).

Тема 9. Протоколи мережевих служб: DNS, DHCP, NTP

Служба імен DNS: ієрархія простору імен, зони, делегування, типи записів (A, AAAA, MX, NS, CNAME, TXT, PTR). Ітеративні та рекурсивні запити, кешування, поле TTL. Формат повідомлень DNS, поле Transaction ID. Розширення DNSSEC; транспорт DoH і DoT. Атаки: підміна відповідей, отруєння кешу, DNS-тунелювання, підсилення. Протокол DHCP: процедура DORA, параметри та опції, ретрансляція, резервування адрес; DHCPv6. Загроза підставного

сервера DHCP та механізм DHCP snooping. Протокол NTP: ієрархія стратумів, режими роботи, автентифікація, зловживання для атак підсилення. Значення синхронізації часу для журналювання та розслідування інцидентів.

Тема 10. Протоколи веб-служб та обміну даними між застосунками

Протокол HTTP/1.1: методи, коди стану, структура заголовків, збереження стану через cookie, постійні з'єднання. Протокол HTTP/2: двійкове кадрування, мультиплексування потоків, стиснення заголовків HPACK, надсилання сервером. Протокол HTTP/3 поверх QUIC. Архітектурний стиль REST: ресурси, методи, версіонування, документування (OpenAPI). Виклик віддалених процедур gRPC і формат Protocol Buffers. Протокол WebSocket для двоспрямованого обміну. Автентифікація й авторизація доступу до програмних інтерфейсів: ключі, токени, OAuth 2.0, JWT. Обмеження інтенсивності запитів. Типові вразливості вебпротоколів та інтерфейсів (перелік OWASP API Security).

Тема 11. Протоколи електронної пошти та передавання файлів

Архітектура системи електронної пошти: агенти MUA, MTA, MDA. Протокол SMTP і його розширення ESMTP: команди, коди відповідей, ретрансляція, ризик відкритого релея. Протоколи доступу до поштових скриньок POP3 та IMAP. Стандарт MIME і кодування вкладень. Захист електронної пошти: STARTTLS, механізми SPF, DKIM і DMARC; підміна відправника як основа фішингових кампаній. Протоколи передавання файлів: FTP (активний і пасивний режими, окремі з'єднання керування й даних), FTPS, SFTP на базі SSH, TFTP та його застосування в мережевому обладнанні. Порівняння протоколів за захищеністю.

Тема 12. Протоколи бездротових мереж та Інтернету речей

Архітектура WLAN: BSS, ESS, точка доступу, контролер. Стандарти IEEE 802.11a/b/g/n/ac/ax (Wi-Fi 6/6E) і перспективи 802.11be. Метод доступу CSMA/CA, кадри керування та службові кадри, процедури сканування, автентифікації й асоціації. Еволюція механізмів захисту: WEP, WPA, WPA2 (PSK та Enterprise), WPA3 (SAE, OWE), захист службових кадрів 802.11w. Протокол контролю доступу IEEE 802.1X, методи EAP та взаємодія із сервером RADIUS. Типові атаки: rogue AP, evil twin, деавтентифікація, перехоплення рукостискання. Протоколи Інтернету речей: MQTT (публікація та підписка, рівні QoS, автентифікація), CoAP, огляд LoRaWAN; характерні проблеми захищеності IoT-протоколів.

Тема 13. Криптографічні протоколи захищеного передавання даних

Завдання криптографічних протоколів: автентифікація сторін, узгодження ключів, конфіденційність і цілісність даних. Протокол TLS 1.3: етапи рукостискання, набори шифрів, сертифікати та інфраструктура відкритих ключів, відмінності від TLS 1.2. Архітектура IPsec: протоколи AH та ESP, транспортний і тунельний режими, асоціації безпеки, протокол узгодження ключів IKEv2. Протокол WireGuard: принципи побудови, переваги та обмеження. Протокол SSH: версії, автентифікація за ключами, прокидання портів і тунелювання. Порівняння протоколів за продуктивністю та стійкістю. Перспективи впровадження постквантових алгоритмів у протоколи захищеного передавання.

Тема 14. Протоколи керування та моніторингу мережі

Завдання керування мережею: конфігурування, контроль стану, облік, виявлення несправностей. Протокол SNMP: версії v1, v2c та v3, база керувальних даних MIB, ідентифікатори OID, операції get, set, trap та inform; недоліки захищеності ранніх версій і механізми SNMPv3. Протокол syslog: рівні важливості, категорії, транспорт, захист журналів від підміни. Потокові протоколи NetFlow, IPFIX і sFlow: склад запису потоку, архітектура «експортер — колектор», застосування для виявлення аномалій. Протоколи програмного конфігурування NETCONF і RESTCONF, модель даних YANG. Автоматизація адміністрування мережі та її вплив на безпеку.

Тема 15. Аналіз мережевих протоколів для потреб кібербезпеки. Сучасні тенденції

Методика аналізу протоколів: зіставлення реалізації зі специфікацією, виявлення відхилень від документів RFC, тестування граничних значень і фазинг протокольних реалізацій. Пошук і усунення несправностей за рівнями моделі OSI; інструменти діагностування (ping, traceroute, dig, ss, tcpdump, Wireshark, nmap). Класифікація атак на протоколи: підміна, повторне відтворення,

зниження версії, виснаження ресурсів, тунелювання в дозволених протоколах. Аналіз шифрованого трафіку за метаданими. Профілювання нормальної поведінки протоколів та виявлення аномалій. Програмно-конфігуровані мережі (SDN) і протокол OpenFlow, віртуалізація мережевих функцій (NFV). Архітектура нульової довіри (NIST SP 800-207). Тенденції розвитку протоколів: шифрування за замовчуванням, скорочення рукостискань, перехід до QUIC.

9. Опис ІЗ/КПІЗ

Індивідуальні завдання з дисципліни «Мережеві технології та протоколи» виконується самостійно кожним студентом. КПІЗ охоплює усі основні теми дисципліни «Мережеві технології та протоколи».

Метою виконання КПІЗ є оволодіння навичками застосування теоретичних знань. КПІЗ оформлюється у відповідності з встановленими вимогами. Виконання КПІЗ є одним із обов'язкових складових модулів залікового кредиту з дисципліни «Мережеві технології та протоколи».

Індивідуальне завдання оцінюється за 100-бальною шкалою. Виконання індивідуального завдання є одним із обов'язкових складових модулів залікового кредиту з дисципліни «Мережеві технології та протоколи».

Тематика	**Обсяг**	**Вимоги до виконання**
«Проєктування мережі підприємства та обґрунтування вибору мережевих протоколів» за індивідуальним варіантом вихідних даних (тип підприємства, кількість підрозділів і робочих місць, серверів і сервісів, філій, базова мережа IPv4 і префікс IPv6, вимоги до бездротового доступу, резервування та безпеки). Робота охоплює: аналіз вимог; вибір топології та ієрархічної моделі мережі; сегментацію на VLAN; розрахунок IP-адресації (VLSM для IPv4, план IPv6); вибір і обґрунтування протоколів канального, мережевого та прикладного рівнів (802.1Q, STP/RSTP, LACP, OSPF, DHCP, DNS, NAT, SSH, SNMPv3, WPA3); заходи мережевої безпеки (ACL, захист портів, DHCP Snooping); моделювання та перевірку мережі в середовищі емуляції	Пояснювальна записка 20–30 сторінок формату А4 без урахування додатків; графічна частина 3–5 рисунків (логічна і фізична схеми мережі, топологія в середовищі емуляції); таблиці адресації та VLAN; конфігурації пристроїв у додатках; файл проєкту мережі (.pkt / .gns3)	Робота виконується самостійно за своїм варіантом (номер у списку групи). Моделювання виконується в середовищі емуляції (Cisco Packet Tracer, GNS3 або EVE-NG). Розрахунки адресації наводяться повністю з поясненнями. Вибір кожного протоколу обґрунтовується порівнянням з альтернативами. Працездатність мережі підтверджується результатами перевірки (ping, traceroute, show-команди). Оформлення: Times New Roman 14 пт, інтервал 1,5, поля 25/20 мм; рисунки й таблиці пронумеровані та підписані; список джерел за ДСТУ 8302:2015, джерела не старіші за 5 років. Робота подається у встановлений термін і захищається демонстрацією моделі мережі та відповідями на запитання

10. Загальні вимоги

Освітній процес регулюється академічними правилами ЛНТУ. Здобувачі освіти зобов’язані ознайомитися з вимогами, визначеними Кодексом академічної доброчесності ЛНТУ та Політикою етичного використання штучного інтелекту в ЛНТУ, і дотримуватися принципів академічної доброчесності та етичного використання штучного інтелекту в освітній діяльності.

Академічна доброчесність. Учасники освітнього процесу зобов’язані дотримуватися Закону України «Про академічну доброчесність» від 18.12.2025 № 4742-IX та внутрішніх нормативних документів ЛНТУ. Не допускаються академічний плагіат, фабрикація, фальсифікація,

привласнення авторства, несамостійне виконання завдань, а також недоброчесне використання результатів, згенерованих штучним інтелектом.

Використання штучного інтелекту. Інструменти штучного інтелекту можуть використовуватися для пошуку ідей, пояснення методів, попереднього структурування, мовного редагування та допоміжного аналізу неконфіденційних даних, якщо конкретне завдання не передбачає повністю самостійного виконання. Здобувач освіти має зазначати використаний інструмент, мету та етап його застосування, перевіряти факти й розрахунки та самостійно обґрунтовувати висновки.

11. Література

I. Навчально-методичні матеріали та розробки

Праці інших авторів:

1. Задерейко О. В., Багнюк Н. В., Толокнов А. А. Комп'ютерні мережі : навчально-методичний посібник. Одеса : Фенікс, 2023. 211 с.

2. Чепинога А. В., Єфіменко А. А., Рудаков К. С., Лавданський А. О., Ланських Є. В., Фауре Е. В. Комп'ютерні мережі : навч. посіб. Житомир : Житомирська політехніка, 2025. 386 с.

3. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 8th ed. Harlow : Pearson, 2021. 832 p.

4. Tanenbaum A. S., Feamster N., Wetherall D. Computer Networks. 6th ed. Harlow : Pearson, 2021. 944 p.

5. Odom W. CCNA 200-301 Official Cert Guide, Volume 1. 2nd ed. Indianapolis : Cisco Press, 2024. 944 p.

II. Наукові праці

Праці автора силабуса:

6. Римчук І., Костючко С., Поліщук М., Гринюк С., Конкевич Л. Безпека комунікаційних процесів з використанням візуальної криптографії. Кібербезпека: освіта, наука, техніка. 2024. № 2(26). С. 258–267. URL: https://repository.lntu.edu.ua/handle/123456789/4595

III. Інформаційні ресурси

7. Офіційний ресурс IETF (документи RFC). URL: https://www.rfc-editor.org

8. Стандарти IEEE 802 (LAN/MAN Standards Committee). URL: https://standards.ieee.org/ieee/802/

9. Cisco Networking Academy (курси CCNA, актуальна редакція). URL: https://www.netacad.com

10. Wireshark: документація та навчальні матеріали. URL: https://www.wireshark.org/docs/

11. OWASP API Security Project. URL: https://owasp.org/www-project-api-security/

12. ENISA Threat Landscape: щорічні аналітичні звіти. URL: https://www.enisa.europa.eu

13. Матеріали Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua

14. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA. URL: https://cert.gov.ua