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

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

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

СИЛАБУС

з освітнього компонента «Техніки захисту і протидії мережевим атакам»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека та захист інформації
освітня програма – Кібербезпека

Кафедра кібербезпеки

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

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/2332

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Техніки захисту і протидії мережевим атакам»

Освітня програма	Кібербезпека
Галузь знань / Спеціальність	12 Інформаційні технології / 125 Кібербезпека та захист інформації
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	нормативна
Мова викладання	українська
Обсяг	5 кредитів ECTS / 150 годин, семестр 7
Форма контролю	екзамен, курсова робота
Викладач(і)	к.т.н., доцент Сергій КОСТЮЧКО

1. Мета і завдання дисципліни

Мета: Формування у здобувачів вищої освіти теоретичних знань і практичних навичок щодо виявлення, аналізу та протидії мережевим атакам, застосування сучасних методів і засобів захисту комп’ютерних мереж, налаштування механізмів мережевої безпеки та забезпечення захищеності інформаційно-комунікаційних систем.

Завдання: Ознайомлення з основними видами мережевих атак, принципами їх реалізації та можливими наслідками для інформаційно-комунікаційних систем.
Вивчення сучасних методів і технік виявлення, аналізу та запобігання мережевим атакам.
Набуття практичних навичок налаштування та використання міжмережевих екранів, систем виявлення і запобігання вторгненням (IDS/IPS) та інших засобів мережевого захисту.
Опанування методів аналізу мережевого трафіку, виявлення вразливостей і підозрілої активності в комп’ютерних мережах.
Формування навичок застосування захисних механізмів, реагування на мережеві атаки та оцінювання ефективності заходів протидії кіберзагрозам.

Пререквізити: Комп'ютерні мережі, Безпека інформаційно-комунікаційних систем, Системи моніторингу комп'ютерних систем та мереж, Обробка інцидентів та реагування, Аналітик кібербезпеки

2. Компетентності

СК02 — Здатність до використання інформаційно комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК05 — Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК08 — Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

СК12 — Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

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. Сучасні мережеві загрози та технології захисту мережевої інфраструктури								

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
1	Тема 1. Сучасні загрози мережевої безпеки	2/0,5	2/0,5	6/12	10/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК12
2	Тема 2. Забезпечення безпеки мережевих пристроїв	2/–	2/0,5	6/12	10/12,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
3	Тема 3. Автентифікація, авторизація та облік	2/–	2/1	6/12	10/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК12, СК08
4	Тема 4. Впровадження технологій міжмережевого екранування	2/0,5	2/1	6/12	10/13,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК12
5	Тема 5. Впровадження систем запобігання вторгненням	4/–	4/1	12/12	20/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
6	Тема 6. Безпека локальної мережі (LAN)	4/–	4/1	12/12	20/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК12
Змістовий модуль 2. Криптографічний захист, технології VPN та управління безпекою комп'ютерних мереж								
7	Тема 7. Криптографічні системи	2/–	2/1	6/12	10/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК12
8	Тема 8. Використання віртуальних приватних мереж (VPN)	4/–	4/1	12/12	20/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК12
9	Тема 9. Використання багатофункціонального пристрою захисту	2/0,5	2/1	6/14	10/15,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
10	Тема 10. Багатофункціональний пристрій безпеки з розширеним функціоналом	2/–	2/1	6/14	10/15	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
11	Тема 11. Управління безпечною мережею	4/0,5	4/1	12/14	20/15,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК08, СК02, СК05, СК12
	Разом	**30/2**	**30/10**	**90/138**	**150/150**			

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; МО5 — командні проєкти.

4. Результати навчання

ПРН05. адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

ПРН14. вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

ПРН18. використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

ПРН19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

ПРН22. вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційнотелекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

ПРН26. впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;

ПРН27. вирішувати задачі захисту потоків даних в інформаційних, інформаційнотелекомунікаційних (автоматизованих) системах;

ПРН28. аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;

ПРН41. забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

ПРН42. впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;

ПРН46. здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-

телекомунікаційних системах;

ПРН47. вирішувати задачі захисту інформації, що обробляється в інформаційнотелекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;

ПРН48. виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційнотелекомунікаційних системах;

ПРН49. забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;

5. Цілі сталого розвитку

ЦСР 9 – Промисловість, інновації та інфраструктура

ЦСР 16 – Мир, справедливість та сильні інститути

ЦСР 17 – Партнерство заради сталого розвитку

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 (25 %) + модульний контроль (20 %) + курсова робота (15 %) + 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. Сучасні загрози мережевої безпеки

Поняття та класифікація загроз мережевої безпеки. Основні види мережевих атак. Загрози безпеці локальних, корпоративних, хмарних і віртуальних мереж. Архітектура та топології комп'ютерних мереж. Виявлення вразливостей мережевої інфраструктури. Атаки типу DoS та DDoS, їх різновиди та принципи реалізації. Методи виявлення та протидії DDoS-атакам. Принципи багаторівневого захисту мережі. Політика мережевої безпеки. Основи використання концепції Network Foundation Protection (NFP). Оцінювання ризиків мережевої безпеки.

Тема 2. Забезпечення безпеки мережевих пристроїв

Основні принципи захисту мережевого обладнання. Загрози безпеці маршрутизаторів і комутаторів. Захист адміністративного доступу до мережевих пристроїв. Використання захищених протоколів керування. Налаштування облікових записів та адміністративних ролей. Розмежування привілеїв користувачів. Захист конфігурацій мережевого обладнання. Моніторинг стану та керування мережевими пристроями. Протоколи SNMP, SNMPv3 та NTP. Автоматизація налаштувань безпеки. Захист площин керування, контролю та передавання даних. Використання Control Plane Policing (CoPP). Резервне копіювання та відновлення конфігурацій мережевих пристроїв.

Тема 3. Автентифікація, авторизація та облік

Основні принципи ідентифікації та автентифікації користувачів. Концепція AAA (Authentication, Authorization, Accounting). Призначення та функції компонентів AAA. Локальна автентифікація користувачів. Серверна автентифікація та централізоване керування доступом. Протоколи

RADIUS і TACACS+. Налаштування AAA на мережевих пристроях. Авторизація адміністративних команд. Розмежування прав доступу. Облік дій користувачів та адміністраторів. Журналювання подій автентифікації. Багатофакторна автентифікація. Перевірка ефективності механізмів AAA.

Тема 4. Впровадження технологій міжмережевого екранування

Поняття та призначення міжмережевих екранів. Класифікація міжмережевих екранів. Пакетна фільтрація та контроль стану з'єднань. Міжмережеві екрани прикладного рівня. Брандмауери нового покоління (NGFW). Списки контролю доступу (ACL). Стандартні та розширені ACL. Принципи створення правил фільтрації мережевого трафіку. Зональна модель мережевої безпеки. Міжмережевий екран на основі зональних політик (Zone-Based Firewall, ZBF/ZFW). Налаштування зон безпеки. Контроль вхідного та вихідного трафіку. Перевірка ефективності правил міжмережевого екранування.

Тема 5. Впровадження систем запобігання вторгненням

Поняття та призначення систем виявлення і запобігання вторгненням (IDS/IPS). Класифікація IDS/IPS. Мережеві та хостові системи виявлення вторгнень. Принципи сигнатурного та поведінкового аналізу. Методи виявлення мережевих аномалій. Сигнатури атак та правила виявлення загроз. Режими функціонування IDS та IPS. Основи впровадження мережевих IPS. Використання систем Snort і Suricata. Налаштування правил виявлення мережевих атак. Аналіз сповіщень IDS/IPS. Хибнопозитивні та хибнонегативні спрацювання. Оцінювання ефективності систем запобігання вторгненням.

Тема 6. Безпека локальної мережі (LAN)

Основні загрози безпеці локальних комп'ютерних мереж. Захист мережевої інфраструктури LAN. Безпека кінцевих пристроїв. Захист комутаторів другого рівня моделі OSI. Основні види атак канального рівня. MAC Flooding, ARP Spoofing та VLAN Hopping. Захист від атак на DHCP. Технології Port Security, DHCP Snooping, Dynamic ARP Inspection та IP Source Guard. Сегментація локальної мережі за допомогою VLAN. Захист магістральних з'єднань. Безпека протоколу Spanning Tree. Контроль доступу до мережі за стандартом IEEE 802.1X. Моніторинг та виявлення підозрілої активності в локальній мережі.

Тема 7. Криптографічні системи

Основні поняття криптографічного захисту інформації. Принципи забезпечення конфіденційності, цілісності та автентичності даних. Симетричні та асиметричні криптографічні системи. Алгоритми симетричного шифрування AES. Криптографія відкритого ключа. Алгоритми RSA та криптографія на еліптичних кривих. Криптографічні хеш-функції. Механізми контролю цілісності інформації. Коди автентифікації повідомлень (MAC, HMAC). Електронні цифрові підписи. Інфраструктура відкритих ключів (PKI). Цифрові сертифікати X.509. Принципи управління криптографічними ключами. Використання криптографічних механізмів у мережевих протоколах безпеки.

Тема 8. Використання віртуальних приватних мереж (VPN)

Поняття та призначення віртуальних приватних мереж. Основні типи VPN. Принципи тунелювання та шифрування мережевого трафіку. Архітектура VPN-з'єднань. Технології Site-to-Site VPN та Remote Access VPN. Протоколи IPsec, IKEv2 та SSL/TLS. Основні компоненти IPsec. Протоколи AH та ESP. Режими функціонування IPsec. Узгодження параметрів криптографічного захисту. Налаштування Site-to-Site IPsec VPN за допомогою командного рядка (CLI). Використання криптографічних карт (Crypto Maps). Перевірка працездатності VPN-тунелів. Аналіз безпеки VPN-з'єднань.

Тема 9. Використання багатофункціонального пристрою захисту

Призначення та функціональні можливості пристроїв Cisco Adaptive Security Appliance (ASA). Архітектура та основні компоненти Cisco ASA. Режими функціонування міжмережевого екрана. Основи конфігурування Cisco ASA. Налаштування мережевих інтерфейсів і зон безпеки. Рівні безпеки інтерфейсів. Налаштування маршрутизації. Використання списків контролю доступу. Налаштування трансляції мережевих адрес (NAT/PAT). Керування адміністративним доступом.

Моніторинг стану пристрою. Перевірка правил фільтрації та аналіз мережевого трафіку.

Тема 10. Багатофункціональний пристрій безпеки з розширеним функціоналом

Розширені можливості Cisco Adaptive Security Appliance. Засоби централізованого адміністрування міжмережевих екранів. Використання Cisco Adaptive Security Device Manager (ASDM). Налаштування політик мережевої безпеки через графічний інтерфейс. Розширена фільтрація мережевого трафіку. Налаштування об'єктів і груп мережевих ресурсів. Основи організації VPN на пристроях Cisco ASA. Налаштування IPsec Site-to-Site VPN. Налаштування віддаленого VPN-доступу. Управління сертифікатами та криптографічними ключами. Моніторинг VPN-з'єднань. Діагностика несправностей і перевірка ефективності конфігурацій безпеки.

Тема 11. Управління безпечною мережею

Основні принципи управління безпекою комп'ютерних мереж. Організація процесів мережевого адміністрування. Політики інформаційної та мережевої безпеки. Структура та зміст політики безпеки організації. Управління доступом до мережевих ресурсів. Моніторинг мережевої активності та стану обладнання. Централізоване збирання та аналіз журналів подій. Використання Syslog і SNMP для контролю мережевої інфраструктури. Управління конфігураціями мережевих пристроїв. Оцінювання вразливостей і ризиків мережевої безпеки. Реагування на інциденти мережевої безпеки. Аудит налаштувань мережевого обладнання. Оцінювання ефективності політик та механізмів захисту комп'ютерних мереж.

9. Курсова робота

Курсова робота з дисципліни спрямована на закріплення теоретичних знань і формування практичних навичок захисту інформації, аналізу мережевих загроз, застосування програмних і програмно-апаратних засобів захисту, а також відновлення функціонування інформаційно-комунікаційних систем після кіберінцидентів. Тематика курсових робіт передбачає дослідження методів захисту інформації, аналіз мережевих атак, розроблення та налаштування механізмів безпеки комп'ютерних мереж, оцінювання ефективності засобів захисту та забезпечення відмовостійкості ІКС.

Обсяг пояснювальної записки становить 20-30 сторінок друкованого тексту без урахування додатків. Курсова робота повинна містити титульний аркуш, завдання, зміст, вступ, основну частину (теоретичний, практичний та аналітичний розділи), висновки, список використаних джерел і додатки (за необхідності).

Курсова робота виконується індивідуально відповідно до затвердженої теми. Здобувач повинен проаналізувати предметну область, обґрунтувати вибір методів і засобів захисту, виконати практичне завдання з налаштування, моделювання або дослідження безпеки ІКС, провести аналіз отриманих результатів та сформулювати висновки.

Пояснювальна записка оформлюється на аркушах формату А4 відповідно до методичних рекомендацій закладу вищої освіти. Параметри: шрифт Times New Roman, розмір 14 пт, міжрядковий інтервал 1,5; поля: ліве — 30 мм, праве — 10 мм, верхнє та нижнє — 20 мм. Рисунки, таблиці, формули та використані джерела оформлюються відповідно до встановлених вимог.

Захист курсової роботи передбачає коротку доповідь здобувача (5–7 хвилин), презентацію основних результатів, демонстрацію практичної частини (за наявності) та відповіді на запитання. Оцінювання здійснюється з урахуванням повноти розкриття теми, правильності технічних рішень, якості практичної реалізації, самостійності виконання та обґрунтованості висновків.

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 автора силабуса:

1. IoT-технології для кіберфізичних систем: конспект лекцій для здобувачів другого (магістерського) рівня вищої освіти освітньої програми «Комп’ютерна інженерія» галузь знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія денної та заоч. форм навч. / уклад. С. В. Гринюк. Луцьк: ЛНТУ, 2026. 48 с. URL: https://repository.lntu.edu.ua/handle/123456789/4406

2. Програмування на Python: метод. вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 (F) Інформаційні технології денної та заоч. форм навч. / уклад.: С. М. Костючко, Л. М. Конкевич. Луцьк: ЛНТУ, 2026. 60 с. URL: https://repository.lntu.edu.ua/handle/123456789/3352

II. Наукові праці

Праці автора силабуса:

3. Tkachuk A., Polishchuk M., Polishchuk L., Kostiuchko S., Hryniuk S., Konkevych L. Investigation of DC-AC converter with microcontroller control of inverter frequency. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2025. Vol. 15, No. 1. P. 55–61. URL: https://repository.lntu.edu.ua/handle/123456789/2012.

4. Bahniuk N., Terletskyi T., Kaidyk O., Kostiuchko S., Kondius I. Solving operational tasks in the design of video surveillance systems. CEUR Workshop Proceedings : Applied Information Technologies and Artificial Intelligence Systems. 2025. P. 332–342. URL: https://ceur-ws.org/Vol-4160/paper20.pdf.

5. Khrystynets N., Melnyk K., Lavrenchuk S., Miskevych O., Kostiuchko S. Multiprocessing as a Way to Optimize Queries. Advances in Transdisciplinary Engineering. 2024. No. 48. P. 455–464. DOI: https://doi.org/10.3233/ATDE231357.

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.

7. Каган І., Костючко С. CRM-системи як інструмент підвищення ефективності бізнесу. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2023. № 52. С. 5–9. DOI: https://doi.org/10.36910/6775-2524-0560-2023-52-01.

8. Polishchuk M., Grinyuk S., Kostiuchko S., Tkachuk A., Savaryn P. Tesla Switch of 4 Batteries Based on the Arduino Uno Board. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2023. Vol. 13, No. 3. P. 111–116. DOI: https://doi.org/10.35784/iapgos.4051.

9. Kostiuchko S., Polishchuk M., Zabolotnyi O., Tkachuk A., Twarog B. The Auxiliary Parametric Sensitivity Method as a Means of Improving Project Management Analysis and Synthesis of Executive Elements. Emerging Technologies in Computing / eds. M. H. Miraz, G. Southall, M. Ali, A. Ware, S. Soomro. Cham : Springer, 2021. (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering ; vol. 395). P. 92–103. DOI:

https://doi.org/10.1007/978-3-030-90019-9_8.

10. Kostiuchko S., Kyryliuk L., Chernyashchuk N., Bortnyk K., Hrunjuk S. Wireless access point with multilayer data protection algorithm. Computer-integrated technologies: education, science, production. 2021. No. 42. P. 147–151. DOI: https://doi.org/10.36910/6775-2524-0560-2021-42-21.

11. Костючко С. М., Багнюк Н. В., Кузьмич О. І., Поліщук М. М., Кирилюк Л. М. Біометрична ідентифікація засобами Python та Raspberry Pi. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2021. Вип. 42. С. 142–146. DOI: https://doi.org/10.36910/6775-2524-0560-2021-42-20.

Праці інших авторів:

12. Santos O. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide. 2nd ed. Indianapolis : Cisco Press, 2023. 832 p. URL: https://www.ciscopress.com/store/ccnp-and-ccie-security-core-scor-350-701-official-cert-9780138221263.

13. Musa S. M. Network Security and Cryptography : A Comprehensive Guide to Network Protection and Encryption Techniques. Boston : Mercury Learning and Information, 2024. 611 p. URL: https://www.packtpub.com/en-us/product/network-security-and-cryptography-9781836641568.

14. Singh G. D. The Ultimate Kali Linux Book : Harness Nmap, Metasploit, Aircrack-ng, and Empire for Cutting-Edge Pentesting. 3rd ed. Birmingham : Packt Publishing, 2024. 828 p. URL: https://www.packtpub.com/en-us/product/the-ultimate-kali-linux-book-9781835083680.

15. Neil I. CompTIA Security+ SY0-701 Certification Guide : Master Cybersecurity Fundamentals and Pass the SY0-701 Exam on Your First Attempt. 3rd ed. Birmingham : Packt Publishing, 2024. 634 p. URL: https://www.packtpub.com/en-us/product/comptia-security-sy0-701-certification-guide-9781835461532.

16. Mukherjee A. The Complete Guide to Defense in Depth. Birmingham : Packt Publishing, 2024. URL: https://www.oreilly.com/library/view/the-complete-guide/9781835468265/.