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 «Безпека інформаційно-комунікаційних систем»
ступінь вищої освіти – бакалавр
галузь знань – F Інформаційні технології
спеціальність – F5 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/2323

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Безпека інформаційно-комунікаційних систем»

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 4
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 забезпечення безпеки інформаційно-комунікаційних систем, виявлення та аналізу кіберзагроз, оцінювання вразливостей, застосування сучасних методів і засобів захисту інформації, моніторингу подій безпеки та реагування на кіберінциденти для забезпечення конфіденційності, цілісності й доступності інформаційних ресурсів.

Завдання: Ознайомлення з основними принципами та методами захисту інформації, що обробляється і зберігається в інформаційно-комунікаційних системах.
Вивчення принципів роботи та набуття навичок використання програмних і програмно-апаратних засобів захисту інформації.
Опанування методів відновлення працездатності інформаційно-комунікаційних систем після кібератак, збоїв та відмов.
Вивчення основних видів мережевих атак, способів їх виявлення та запобігання.
Набуття практичних навичок налаштування та використання механізмів безпеки комп’ютерних мереж.

Пререквізити: Програмування та реверс-інжиніринг, Основи кібербезпеки, Алгоритми захисту інформації та системне програмування

2. Компетентності

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

ЗК06 — Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.

СК04 — Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК09 — Здатність застосовувати методи та засоби технічного захисту інформації на об’єктах інформаційної діяльності.

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. Захист інформації та забезпечення стійкості інформаційно-комунікаційних систем								

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
1	Тема 1. Захист інформації, що обробляється та зберігається в ІКС	6/0,5	6/2	24/32	36/34,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5, МО7	ЗК06, СК04, СК09
2	Тема 2. Програмні та програмно-апаратні комплекси ЗЗІ	6/–	6/2	24/34	36/36	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5, МО7	ЗК06, СК04, СК09
3	Тема 3. Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження	6/0,5	6/2	24/34	36/36,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5, МО7	ЗК06, СК04, СК09
Змістовий модуль 2. Мережеві атаки та механізми захисту комп'ютерних мереж								
4	Тема 4. Моніторинг процесів функціонування ІКС	6/0,5	6/2	24/34	36/36,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5, МО7	ЗК06, СК04, СК09
5	Тема 5. Механізми безпеки комп'ютерних мереж	6/0,5	6/2	24/34	36/36,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5, МО7	ЗК06, СК04, СК09
	Разом	**30/2**	**30/10**	**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; МО5 — командні проєкти; МО7 — презентації результатів виконаних завдань та досліджень.

4. Результати навчання

ПРН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

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

ЦСР 16 – Мир, справедливість та сильні інститути

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. Захист інформації, що обробляється та зберігається в ІКС

Основні поняття та принципи захисту інформації в інформаційно-комунікаційних системах. Види інформації та вимоги до її захисту. Загрози конфіденційності, цілісності та доступності інформації. Методи і засоби захисту даних. Ідентифікація, автентифікація та авторизація користувачів. Розмежування прав доступу до інформаційних ресурсів. Криптографічний захист інформації. Захист даних під час зберігання та передавання. Резервне копіювання інформації. Контроль цілісності даних.

Тема 2. Програмні та програмно-апаратні комплекси ЗЗІ

Поняття та класифікація засобів захисту інформації. Програмні, апаратні та програмно-апаратні засоби захисту. Антивірусні програми та системи захисту кінцевих пристроїв. Міжмережеві екрани та їх призначення. Системи виявлення та запобігання вторгненням (IDS/IPS). Засоби контролю доступу. Системи криптографічного захисту інформації. Апаратні засоби автентифікації. Засоби моніторингу інформаційної безпеки. Принципи встановлення, налаштування та використання комплексів захисту інформації. Оцінювання ефективності засобів захисту.

Тема 3. Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження

Основні причини порушення функціонування інформаційно-комунікаційних систем. Класифікація збоїв, відмов та кіберінцидентів. Поняття відмовостійкості та безперервності роботи ІКС. Методи резервного копіювання та відновлення даних. Створення резервних копій операційних систем і конфігурацій мережевого обладнання. Відновлення працездатності серверів та мережевих служб. Планування аварійного відновлення (Disaster Recovery). Показники RPO та RTO. Основні етапи реагування на інциденти. Перевірка працездатності ІКС після відновлення. Аналіз причин збоїв та запобігання їх повторенню.

Тема 4. Моніторинг процесів функціонування ІКС

Поняття та класифікація мережевих атак. Основні загрози безпеці комп'ютерних мереж. Методи мережевої розвідки та сканування. Атаки на мережеві протоколи та служби. Атаки типу DoS та DDoS. Перехоплення мережевого трафіку. Атаки Man-in-the-Middle (MITM). Підміна мережевих адрес (ARP Spoofing, IP Spoofing). Атаки на DNS та DHCP. Атаки на механізми автентифікації. Поширення шкідливого програмного забезпечення через мережу. Методи виявлення мережевих

атак. Аналіз мережевого трафіку за допомогою Wireshark. Ознаки та індикатори мережевих атак.

Тема 5. Механізми безпеки комп'ютерних мереж

Основні принципи забезпечення мережевої безпеки. Методи захисту мережевої інфраструктури. Міжмережеві екрани та правила фільтрації трафіку. Списки контролю доступу (ACL). Сегментація мережі за допомогою VLAN. Захист мережевих пристроїв та служб. Використання віртуальних приватних мереж (VPN). Протоколи захищеного передавання даних TLS, IPsec та SSH. Системи виявлення та запобігання вторгненням (IDS/IPS). Захист бездротових мереж. Контроль доступу до мережевих ресурсів. Моніторинг мережевої активності. Налаштування та перевірка ефективності механізмів захисту комп'ютерних мереж.

9. Курсова робота

Тематика курсової роботи. Курсова робота з дисципліни «Безпека інформаційно-комунікаційних систем» 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 курсової роботи. Обсяг пояснювальної записки становить 25-35 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).

Вимоги до виконання. 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.

Вимоги до оформлення. 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.

Вимоги до захисту. 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

І. 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

ІІ. 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. Easttom C. Network Defense and Countermeasures : Principles and Practices. 4th ed. Indianapolis : Pearson IT Certification, 2023. URL: https://www.oreilly.com/library/view/network-defense-and/9780138200626/.

13. Brotherston L., Berlin A., Reyor W. F. Defensive Security Handbook. 2nd ed. Sebastopol : O'Reilly Media, 2024. URL: https://www.oreilly.com/library/view/defensive-security-handbook/9781098127237/.

14. Lekkala S., Gurijala P. Security and Privacy for Modern Networks : Strategies and Insights for Safeguarding Digital Infrastructures. New York : Apress, 2024. DOI: https://doi.org/10.1007/979-8-8688-0823-4.

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

16. Tykushin A., Ostrovskaya S. Incident Response for Windows. Birmingham : Packt Publishing, 2024. URL: https://www.oreilly.com/library/view/incident-response-for/9781804619322/.