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 «Безпека програм та даних»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 121 Інженерія програмного забезпечення
освітня програма – Інженерія програмного забезпечення

Кафедра інженерії програмного забезпечення

Силабус склав(ла) професор кафедри інженерії програмного забезпечення, д.т.н., професор Ігор АНДРУЩАК

Силабус затверджений на засіданні кафедри інженерії програмного забезпечення, протокол № 1/1 від «28» серпня 2026 р.

Завідувач кафедри к.т.н., доцент Наталія ЛІЩИНА

Розглянуто та схвалено групою забезпечення освітньої програми «Інженерія програмного забезпечення», протокол № 2 від «28» лютого 2026 р.

Гарант ОП «Інженерія програмного забезпечення» к.т.н., доцент Наталія ЛІЩИНА

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

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/1204

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Безпека програм та даних»

Освітня програма	Інженерія програмного забезпечення
Галузь знань / Спеціальність	12 Інформаційні технології / 121 Інженерія програмного забезпечення
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	нормативна
Мова викладання	українська
Обсяг	4 кредити ECTS / 120 годин, семестр 6
Форма контролю	екзамен
Викладач(і)	д.т.н., професор Ігор АНДРУЩАК

1. Мета і завдання дисципліни

Мета: Метою навчальної дисципліни «Безпека програм та даних» є навчання студентів принципам захисту програмного забезпечення на всьому циклі його існування, дослідженню та використанню сучасних процедур забезпечення основних услуг безпеки інформації в інформаційно-комунікаційних ресурсах Інтернет-технологій та кіберпросторі, що засновані на використанні алгоритмів симетричної та несиметричної криптографії, цифровому підписі та протоколів інфраструктури відкритих ключів (ІВК).

Завдання: Завдання вивчення дисципліни:
- ознайомлення з принципами протоколів обміну даними в кіберпросторі;
- ознайомлення з сучасними програмно-апаратними застосунками забезпечення безпеки персональних даних;
- ознайомлення з правовими аспектами забезпечення інформаційної і кібербезпеки на рівні держави, міжнародному рівні;
- навчитися орієнтуватися в сучасних загрозах, їх направленості;
- навчитися аналізувати ризики використання конфіденційної інформації, відрізняти фейкову інформацію в медіапросторі;
- навчитися орієнтуватися у послугах і механізмах забезпечення безпеки;
- набути практичних здатностей в забезпеченні безпеки особистих персональних даних в умовах сучасних загроз.

Пререквізити: Організація баз даних і знань, Операційні системи

2. Компетентності

ІК — інтегральна компетентність: Здатність розв’язувати складні спеціалізовані завдання або практичні проблеми інженерії програмного забезпечення, що характеризуються комплексністю та невизначеністю умов, із застосуванням теорій та методів інформаційних технологій.

ЗК02 — Здатність застосовувати знання у практичних ситуаціях.

ЗК05 — Здатність вчитися і оволодівати сучасними знаннями.

СК05 — Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу.

СК06 — Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі 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

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
Змістовий модуль 1. Принципи безпеки і захисту програм та даних								
1	Тема 1. Тема 1. Основні поняття безпеки програм та даних.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05, СК06
2	Тема 2. Характеристика сучасних загроз.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05, СК06
3	Тема 3. Безпека зберігання даних в операційних системах.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05, СК06
4	Тема 4. Ідентифікація та аутентифікація користувачів.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05, СК06
5	Тема 5. Центр забезпечення безпеки (Windows Security Center) в операційній системі Windows.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05
6	Тема 6. Захист від шкідливого програмного забезпечення. Windows Defender.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05
7	Тема 7. Захист даних на основі приховування інформації.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05, СК06
8	Тема 8. Захист програм від несанкціонованого дослідження.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05, СК06
Змістовий модуль 2. Мережева безпека								

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
9	Тема 9. Протоколи захисту інформації на мережевому рівні.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05
10	Тема 10. Криптографічний механізми захисту інформації та їх застосування.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05, СК06
11	Тема 11. Цілісність та автентичність даних.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05, СК06
12	Тема 12. Програмно-апаратні (програмні) засоби захисту інформації в мережі Wi-Fi.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05, СК06
13	Тема 13. Методи та засоби обмеження доступу до програм та даних.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05, СК06
14	Тема 14. Віртуальні приватні мережі.	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05, СК06
15	Тема 15. Захист комп’ютерних мереж та персональних комп’ютерів за допомогою брандмауера (Firewall).	2/0,4	2/0,4	4/7,2	8/8	МН1, МН2, МН3, МН4, МН5, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК02, ЗК05, СК05
	Разом	**30/6**	**30/6**	**60/108**	**120/120**			

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); МН6 — самостійна робота (розв’язання завдань).

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

4. Результати навчання

ПРН04. Знати і застосовувати професійні стандарти і інші нормативно правові документи в галузі інженерії програмного забезпечення.

ПРН21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

5. Цілі сталого розвитку

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 (30 %) + модульний контроль (30 %) + 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. Тема 1. Основні поняття безпеки програм та даних.

Предмет і задачі захисту програм і даних. Вразливість комп’ютерних систем. Політика безпеки в комп’ютерних системах. Оцінка та механізми захисту програм та даних. Стандарти захисту даних.

Тема 2. Характеристика сучасних загроз.

Формальне визначення криптосистеми. Критерії та показники ефективності. Аналіз основних видів атак, ризиків та вразливих на елементи інформаційних систем в кіберпросторі. Синергія та гібридність сучасних загроз, основні тенденції спрямованості.

Тема 3. Безпека зберігання даних в операційних системах.

Технологія тіньового копіювання даних. Стратегії архівації (повна архівація, повна архівація з подальшою додатковою, повна архівація з подальшою різницевою, щоденна архівація). Робота з томами RAID. Відновлення даних.

Тема 4. Ідентифікація та аутентифікація користувачів.

Біометрична аутентифікація користувачів. Перевірка автентичності користувачів. Протоколи ідентифікації. Ідентифікація користувачів на основі системи паролів. Вимоги до паролів. Схема зберігання паролів.

Тема 5. Центр забезпечення безпеки (Windows Security Center) в операційній системі Windows.

Три основні компоненти безпеки ОС: брандмауер, антивірус, система автоматичного оновлення. Параметри безпеки. Налаштування безпеки браузера. Створення виключення для програми.

Тема 6. Захист від шкідливого програмного забезпечення. Windows Defender.

Технологія безпеки, що захищає комп’ютер від програм-шпигунів і інших видів небажаних програм. Установка Windows Defender, вимоги до системи. Налаштування Windows Defender. Автоматична перевірка (Automatic scanning). Дії за умовчанням (Default actions). Параметри захисту в режимі реального часу (Real-time protection options). Виявлення підозрілих дій.

Тема 7. Захист даних на основі приховування інформації.

Основи цифровій стеганографії. Класифікація методів цифровій стеганографії з відкритим ключем. Основні методи приховування конфіденційної інформації.

Тема 8. Захист програм від несанкціонованого дослідження.

Методи дослідження програмного коду. Засоби дослідження програмного коду. Принципи та підходи щодо захисту програмного коду від несанкціонованого дослідження.

Тема 9. Протоколи захисту інформації на мережевому рівні.

Захист інформації на мережному рівні. Протоколи захисту та цілісності IPSec, SSL, TLS, їх сутність. Системи захисту PGP та CS MIME. Криптографічні функції.

Тема 10. Криптографічний механізми захисту інформації та їх застосування.

Основні поняття та визначання криптографічного захисту інформації. Алгоритми шифрування даних. Сучасні симетричні та асиметричні шифри.

Тема 11. Цілісність та автентичність даних.

Цифровий підпис. Хеш-функції. MAC-коди. Цифрові сертифікати. Цифрові підписи. Технологія Blockchain.

Тема 12. Програмно-апаратні (програмні) засоби захисту інформації в мережі Wi-Fi.

Основні принципи захисту інформації при підключенні до мережі Wi-Fi. Використання паролів і механізмів контролю.

Тема 13. Методи та засоби обмеження доступу до програм та даних.

Вразливість коп’ютерних систем. Способи проникнення до комп’ютерних систем. Спостереження за користувачами КС. Особливості обмеження доступу до програм та даних.

Тема 14. Віртуальні приватні мережі.

Види віртуальних приватних мереж. Сервіси VPN. Способи утворення захищених тунелів. Рівні реалізації VPN.

Тема 15. Захист комп’ютерних мереж та персональних комп’ютерів за допомогою брандмауера (Firewall).

Принципи роботи, можливості, типи міжмережних екранів (МЕ) та їх особливості. Переваги та недоліка встановлення персональних МЕ.

9. Опис ІЗ/КПІЗ

Не передбачено навчальним планом.

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. Андрущак І. Є. Безпека програм та даних. Конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти програми «Інженерія програмного забезпечення» галузі знань 12 Інформаційні технології спеціальності 121 «Інженерія програмного забезпечення» денної та заоч. форм навч. Луцьк: ЛНТУ, 2025. 100 с.

2. Андрущак І. Є. Безпека програм та даних. Методичні вказівки до лабораторних занять для здобувачів першого (бакалаврського) рівня вищої освіти програми «Інженерія програмного забезпечення» галузі знань 12 Інформаційні технології спеціальності 121 «Інженерія програмного забезпечення» денної та заоч. форм навч. Луцьк: ЛНТУ, 2024. 82 с.

3. Андрущак І. Є. Безпека програм та даних. Методичні вказівки до виконання самостійної роботи для здобувачів першого (бакалаврського) рівня вищої освіти програми «Інженерія програмного забезпечення» галузі знань 12 Інформаційні технології спеціальності 121 «Інженерія програмного забезпечення» денної та заоч. форм навч. Луцьк: ЛНТУ, 2024. 16 с.

Праці інших авторів:

4. Бевз О. В., Ковтун В. Ю. Кібербезпека в освітньому середовищі: навч. посіб. К.: Літера, 2023. 192 с.

5. Гапак О. М. Комп’ютерна криптографія: навч. посіб. Ужгород: видавництво ПП «АУТДОР-ШАРК», 2021р. 96 с.

6. Горбенко В. І., Лісняк А. О. Безпека програм та даних: навч. посіб. Запоріжжя: ЗНУ, 2022. 72 с.

7. Дем’яненко, В. А., Кузнецова Ю. А. Безпека програм та даних: навч. посіб. Харків: Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т», 2021. 95 с.

8. Євсеєв С. П., Король О. Г. Криптографічний захист інформації: навч. посіб. Х.: ХНЕУ ім. С. Кузнеця, 2022. 245 с.

9. Євсєев С. П., Мілов О. В., Остапов С. Е., Сєвєрінов О. В. Кібербезпека: основи кодування та криптографії: навч. посіб. Харків: Вид. “Новий Світ-2000”, 2023. 657 с.

10. Лахно В. А., Василіу Є. В., Гладких В. М., Домрачев В. М., Сивкова Н. М. Методи та засоби захисту інформації: навч. посіб. К.: ЦП «Компринт». 2021. 444 с.

11. Носок С., Фаль М., Ткач В. Управління інформаційною безпекою: конспект лекцій: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2021. 258 с.

12. Самойлов І. В., Матійко А. А., Сторчак А.С. Криптографія: навч. посіб. КПІ ім. Ігоря Сікорського. Київ, 2023. 372 с.

13. Сілін Є. С., Кадубовський О. А. Основи кібербезпеки: навч. посіб. Дніпро, 2023. 200 с.

14. Смірнов О. А., Конопліцька-Слободенюк О. К., Смірнов С. А. Вступ до кібербезпеки: навч. посіб. Кропивницький: ЦНТУ, 2022. 968 с.

ІІ. Наукові праці

Праці автора силабуса:

15. Андрущак І. Є., Колошко О. В. Метод динамічного розподілу криптографічних операцій між CPU та апаратними прискорювачами. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2026. Вип. 63. С. 130-138. URL: https://repository.lntu.edu.ua/handle/123456789/4613

16. Андрущак І. Є, Кошелюк В. А. Аудит безпеки lightweight kubernetes-кластерів із використанням механізмів довіри на базі multichain. Кібербезпека: освіта, наука, техніка. 2026. Т.

4. № 32. С. 463–477. URL: https://repository.lntu.edu.ua/handle/123456789/5419

17. Andrushchak I., Kosheliuk V. Design of Secure Network Isolation and Trust Models for Multichain Blockchain in Kubernetes. International Journal of Electrical and Computer Engineering Research. 2026. Vol. 6. № 1. P. 11–19. URL: https://repository.lntu.edu.ua/handle/123456789/5420

18. Андрущак І. Є., Шмаровоз С. В. Забезпечення надійності моніторингових систем у корпоративних мережах: типові проблеми і рішення. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2025. Вип. 59. С. 37-42. URL: https://repository.lntu.edu.ua/handle/123456789/5658

19. Андрущак І. Є., Кошелюк В. А., Ясашний Д. Підвищення безпеки контейнерів за допомогою розгортання honeypot. International Science Journal of Engineering Agriculture. 2025. Т. 4. № 3. С. 15–26. URL: https://repository.lntu.edu.ua/handle/123456789/5421

20. Андрущак І. Є., Кошелюк В. А. Окремі аспекти проектування системи інформаційної безпеки для захисту IoT-мереж від атак. International Science Journal of Engineering Agriculture. 2025. Т. 4. № 5. С. 27–39. URL: https://repository.lntu.edu.ua/handle/123456789/5422

21. Андрущак І. Є., Кошелюк В. А., Веремій І. Технології обману в кібербезпеці: інтеграція cowrie та ELK Stack для виявлення атак на мережевий трафік. International Science Journal of Engineering Agriculture. 2025. Т. 4. № 6. С. 1–14. URL: https://repository.lntu.edu.ua/handle/123456789/5423

22. Andrushchak I., Kosheliuk V. Integration of machine learning algorithms for intrusion detection in IoT networks. Actual Issues of Modern Science. Ostrava. 2024. № 32. P. 59–74. URL: https://repository.lntu.edu.ua/handle/123456789/5427

23. Martsenyuk V. P., Sverstyuk A. S., Andrushchak I. Ye., Rechun O. Yu. Components and kay features of the analisis symmetric cryptocircuit. Computer-integrated technologies: education, science, production. 2023. № 50. P. 65-70. URL: https://repository.lntu.edu.ua/handle/123456789/5657

24. Andrushchak I. Ye. Features of the main directions, techniques and methods of protection against fishing attacks. Computer-integrated technologies: education, science, production. 2022. № 47. P. 5-9. URL: https://repository.lntu.edu.ua/handle/123456789/5655

25. Andrushchak I. Ye., Matviiv Yu. Ya., Koshelyuk V. A. Components of viruses and antivirus software in modern information security. Computer-integrated technologies: education, science, production. 2022. № 48. P. 26-30. URL: https://repository.lntu.edu.ua/handle/123456789/5656