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 «Захист операційних систем»
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 Микола ПОЛІЩУК

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/1980

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Захист операційних 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	5 кредитів ECTS / 150 годин, семестр 3
Форма контролю	екзамен
Викладач(і)	к.т.н., доцент Микола ПОЛІЩУК

1. Мета і завдання дисципліни

Мета: Метою викладання курсу "Захист операційних систем" є засвоєння теоретичних основ побудови, принципів проектування, конфігурування й застосування сучасних операційних систем, які забезпечують організацію обчислювальних процесів у корпоративних інформаційних системах економічного, управлінського, виробничого, наукового й іншого призначення, а також надання практичних навичок щодо захисту даних в операційних системах.

Завдання: Освоєння принципів організації безпеки операційних систем персонального комп’ютера; знання основних понять теорії побудови операційних систем; визначення статичних та динамічних характеристик об’єктів архітектури сучасних операційних систем; запобігання шляхів несанкціонованого доступу до даних в операційній системі; вживання заходів протидії проникненню шкідливого програмного забезпечення до операційної системи та відновлення її працездатності після його знешкодження; ознайомлення з методологічними основами розробки та функціонування операційних систем.

Пререквізити: Основи кібербезпеки

2. Компетентності

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

ЗК03 — Здатність спілкуватися державною мовою як усно, так і письмово.

СК01 — Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

СК07 — Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

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. Основи побудови та функціонування операційних систем								
1	Тема 1. Основні поняття операційних систем	2/0,5	2/0,5	8/12	12/13	МН1, МН2, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК03, СК01

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
2	Тема 2. Стандартизація UNIX-подібних операційних систем	4/0,5	4/0,5	8/13	16/14	МН1, МН2, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК03, СК01
3	Тема 3. Підсистема управління процесами.	4/1	4/1	8/13	16/15	МН1, МН2, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК03, СК01, СК07
4	Тема 4. Програмні потоки	2/0,5	2/0,5	8/13	12/14	МН1, МН2, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК03, СК07
5	Тема 5. Керування програмними потоками	2/0,5	2/0,5	8/13	12/14	МН1, МН2, МН6	МО1, МО2, МО4, захист лабораторної роботи, тестування	ЗК03, СК01, СК07
Змістовий модуль 2. Основи безпеки та захисту сучасних операційних систем								
6	Тема 6. Системний підхід до захисту даних в операційних системах	4/0,5	4/0,5	8/13	16/14	МН1, МН2, МН6	МО1, МО2, МО4, захист лабораторної роботи, тестування	ЗК03, СК01, СК07
7	Тема 7. Автентифікація та управління доступом до операційної системи	4/0,5	4/0,5	8/13	16/14	МН1, МН2, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК03, СК01
8	Тема 8. Шкідливе програмне забезпечення в операційних системах	2/0,5	2/0,5	8/12	12/13	МН1, МН2, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК03, СК07
9	Тема 9. Криптопровайдери та захист даних на транспортному рівні	2/0,5	2/0,5	8/13	12/14	МН1, МН2, МН6	МО1, МО2, МО4, захист лабораторної роботи	ЗК03, СК07, СК01

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
10	Тема 10. Стандарти оцінювання безпеки операційних систем. Trustworthy Computing	4/1	4/1	8/13	16/15	МН1, МН2, МН6	МО1, МО2, МО4, тестування, захист лабораторної роботи	ЗК03, СК01, СК07
	ІЗ/КПІЗ			10/10	10/10			
	Разом	**30/6**	**30/6**	**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); МН6 — самостійна робота (розв'язання завдань).

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

4. Результати навчання

ПРН05. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

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 (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. Основні поняття операційних систем

Класифікація операційних систем. Родини операційних систем. Структура операційної системи.

Тема 2. Стандартизація UNIX-подібних операційних систем

Принципи організації UNIX. Архітектура UNIX-подібних операційних систем. ОС як засіб керування ресурсами. Системні основи управління ресурсами. Інтерфейс прикладного програмування. Користувацький інтерфейс. Захист даних і адміністрування. Системні виклики та бібліотечні функції. Стандарти UNIX-подібних операційних систем.

Тема 3. Підсистема управління процесами.

Дисципліни планування процесів – вимоги, показники, класифікація. Базові дисципліни планування.

Тема 4. Програмні потоки

Концепція потоків, їх ідентифікація. Функції керування потоками.

Тема 5. Керування програмними потоками

Засоби синхронізації дій потоків. Взаємні виключення: встановлення та зняття блокування. Запобігання тупиковим ситуаціям. Умовні змінні. Блокування читання-запису.

Тема 6. Системний підхід до захисту даних в операційних системах

Основні завдання забезпечення безпеки. Модель загроз для операційної системи. Монітор безпеки. Підсистема локальної автентифікації. База даних політики Lsass. Диспетчер облікових записів безпеки (SAM).

Тема 7. Автентифікація та управління доступом до операційної системи

Принципи автентифікації і керування доступом. Типи об’єктів, які захищаються. Автентифікація з використанням паролів. Автентифікація з використанням фізичного об'єкта та біометричних даних. Формування списків управління доступом. Реалізація захисту особистих об’єктів. Облікові записи користувачів. Аудит. Загальні принципи організації аудиту. Робота із системним журналом Linux.

Тема 8. Шкідливе програмне забезпечення в операційних системах

Організацій несанкціонованого доступу до даних операційної системи. Атакуюче програмне забезпечення. Віруси. Умовно-небезпечні програми. Троянські коні. Хробаки. Програми-шпигуни. Руткіти. Антивірусні і антиантивірусні технології. Інсайдерські атаки на операційну систему. Атаки, які використовують командний рядок. Атаки, які використовують впровадження програмного коду. Атаки, пов'язані з ескалацією привілеїв.

Тема 9. Криптопровайдери та захист даних на транспортному рівні

Принципи шифрування даних на файлових системах. Створення криптопровайдеру. Гібридні криптосистеми. Цифрові підписи. Електронний підпис бінарних програм. Сертифікати. Шифрувальна файлова система Windows. Захист інформації на мережному рівні. Захист інформації на транспортному рівні.

Тема 10. Стандарти оцінювання безпеки операційних систем. Trustworthy Computing

Критерії оцінювання захищеності операційних систем. Політики безпеки в операційній системі. Міжнародні та відомчі
стандарти оцінювання безпеки операційних систем.

9. Опис ІЗ/КПІЗ

Комплексне практичне індивідуальне завдання (КПІЗ) є видом індивідуальної поза-аудиторної роботи студента. Виконання КПІЗ є одним із обов'язкових складових модулів залікового кредиту з дисципліни «Захист операційних систем». Години для КПІЗ виділені із загальної кількості годин, відведених на самостійну роботу.

Метою виконання КПІЗ є розвиток навичок самостійної роботи, систематизація, узагальнення й закріплення набутих знань для поглибленого вивчення методів діагностики, відновлення, моніторингу й оптимізації складових операційної системи, володіння сервісами безпеки операційних систем. Оволодіння навичками виконання завдань КПІЗ дозволить використовувати набуті знання для потреб подальшого навчального процесу та професійної діяльності.

Завдання для КПІЗ видається студентам в перший тиждень навчання. Вони виконують його самостійно впродовж семестру на основі методичних вказівок до виконання самостійної роботи з дисципліни «Захист операційних систем», опрацьованої літератури, лабораторних занять, конспекту лекцій та зібраної інформації в мережі Інтернет, її аналізу та формулювання висновків. КПІЗ оформляється у відповідно до встановлених вимог. КПІЗ оцінюється за 100-бальною шкалою і складає 10% підсумкового бала з дисципліни

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 інших авторів:

1. Христинець Н.А. Захист операційних систем. Конспект лекцій для здобувачів першого (бакалаврського) рівня освітньо-професійної програми «Кібербезпека» галузь знань 12 «Інформаційні технології» спеціальності 125 Кібербезпека денної та заочної форм навчання. Луцьк : ЛНТУ, 2022. 144 с.

2. Христинець Н.А. Захист операційних систем. Методичні вказівки до лабораторних занять для здобувачів першого (бакалаврського) рівня освітньопрофесійної програми «Кібербезпека» галузь знань 12 «Інформаційні технології» спеціальності 125 Кібербезпека денної та заочної форм навчання. Луцьк : ЛНТУ, 2022. 96 с.

3. Христинець Н.А. Захист операційних систем. Методичні вказівки до виконання самостійної роботи для здобувачів першого (бакалаврського) рівня освітньо-професійної програми «Кібербезпека» галузь знань 12 «Інформаційні технології» спеціальності 125 Кібербезпека денної та заочної форм навчання. Луцьк : ЛНТУ, 2023. 52 с.

4. Дячук С. Ф. Windows 2010 : навчальний посібник. Тернопіль : ТНТУ імені Івана Пулюя, 2021. 144 с.

5. Quick start for Windows Defender – Windows Help. Microsoft Corporation. URL: https://compass-ssl.microsoft.com/assets/3a/fc/3afc799b-8599-435d-bc84-6d4c80ab960a.pdf?n=QS-Defender-overview.pdf (Last accessed: 20.05.2026).

6. Черевик В.М., Танцюра Л.І., Коротков С.С., Сосновий В.О. Операційна ситема Linux : принципи роботи з файловою системою. Київ: ДУТ. 2021. 147 с.

7. Посібник Ubuntu. URL: https://ubunlog.com/uk/керівництво-ubuntu/ (дата звернення: 23.05.2026).

8. PowerShell Documentation. Official product documentation for PowerShell. Microsoft Corporation. URL: https://learn.microsoft.com/enus/powershell/ (Last accessed: 23.05.2026).

9. Полив’яний О.В. Операційна система Windows 10 : електронний навчальний посібник. URL: https://cpto.dp.ua/public_html/posibnyky/OSWin10/zmist.htm (дата звернення: 23.05.2026)

10. Mwiinga P. Operating System. Eden university: Real Deal. 2023. 39p. URL: https://www.researchgate.net/publication/372132620_OPERATING_SYSTEM (Last accessed: 22.05.2026).

11. Windows 10 Step by Step. URL: https://ptgmedia.pearsoncmg.com/images/9780735697959/samplepages/9780735697959.pdf (Last

accessed: 20.05.2026).

12. BASIC VI TUTORIAL. URL:https://www.jics.utk.edu/files/images/csure-reu/PDF-DOC/VI-TUTORIAL.pdf (Last accessed: 20.05.2026)

II. Наукові праці

Праці автора силабуса:

13. Римчук І., Костючко С., Поліщук М., Гринюк С., Конкевич Л. (2024). Безпека комунікаційних процесів з використанням візуальної криптографії. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 258–267.

14. Поліщук, М., Семенюк, О., Поліщук, Л., Ломакін, М. Можливості авторизації та захисту даних користувача під час розробки хмарних веб-додатків для IoT. Науковий журнал «Комп’ютерно-інтегровані технології: освіта, наука, виробництво». Луцьк. 2023 (52), 94-103.

15. Н.А. Христинець, Б.Ю. Овдієвич. Способи резервного копіювання даних в ОС Windows. Збірник тез Всеукраїнської науково-практичної конференції «Theoretical and Applied Cybersecurity» (TACS-2023), м. Київ, КПІ ім. Ігоря Сікорського, 26 травня 2023 року. С.29-30.

16. Христинець Н.А. Журналювання аутентифікації користувачів дистрибутиву Ubuntu. Збірник тез IX Всеукраїнської науково-практичної конференції молодих науковців «Інформаційні технології – 2022». Київ, 19 травня 2022 р. С. 183-185.