**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**
**ФАКУЛЬТЕТ ЦИФРОВИХ, ОСВІТНІХ ТА СОЦІАЛЬНИХ ТЕХНОЛОГІЙ**

**ЗАТВЕРДЖУЮ**
**Декан факультету**
**_____ Галина ГЕРАСИМЧУК**
**«28» серпня 2026 р.**

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

# СИЛАБУС

**з освітнього компонента «Технології захисту інформації»**
**ступінь вищої освіти – бакалавр**
**галузь знань – 01 Освіта/Педагогіка**
**спеціальність – 015.39 Професійна освіта (Цифрові технології)**
**освітня програма – Професійна освіта (комп`ютерні технології)**

**Кафедра цифрових освітніх технологій**

Силабус склав(ла) доцент кафедри цифрових освітніх технологій, к.пед.н., доцент Юлія МЕЛЬНИЧУК

Силабус затверджений на засіданні кафедри цифрових освітніх технологій, протокол № 1а від «28» серпня 2026 р.

Завідувач кафедри к.пед.н., доцент Віталій КАБАК

Розглянуто та схвалено групою забезпечення освітньої програми «Професійна освіта (комп`ютерні технології)», протокол № 1а від «28» серпня 2026 р.

Гарант ОП «Професійна освіта (комп`ютерні технології)» к.пед.н., доцент Віталій КАБАК

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

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/3531

**Луцьк – 2026**

**СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Технології захисту інформації»**

| | |
|---|---|
| **Освітня програма** | Професійна освіта (комп`ютерні технології) |
| **Галузь знань / Спеціальність** | 01 Освіта/Педагогіка / 015.39 Професійна освіта (Цифрові технології) |
| **Рівень вищої освіти** | перший (бакалаврський) |
| **Статус дисципліни** | вибіркова |
| **Мова викладання** | українська |
| **Обсяг** | 5 кредитів ECTS / 150 годин |
| **Форма контролю** | залік |
| **Викладач(і)** | к.пед.н., доцент Юлія МЕЛЬНИЧУК |

**1. Мета і завдання дисципліни**

**Мета:** Формування у здобувачів вищої освіти системи теоретичних знань і практичних умінь щодо організаційних, правових, програмних та технічних засобів захисту інформації, виявлення й оцінювання загроз інформаційній безпеці, запобігання несанкціонованому доступу, забезпечення конфіденційності, цілісності та доступності інформації, а також набуття навичок безпечного використання цифрових технологій, інформаційних систем і сервісів у професійній та освітній діяльності.

**Завдання:** - ознайомлення з основними поняттями, принципами та сучасними підходами до забезпечення інформаційної безпеки;
- формування знань про види інформаційних загроз, вразливостей, ризиків і способи їх виявлення та оцінювання;
- вивчення організаційних, правових, програмних і технічних методів захисту інформації;
- ознайомлення з нормативно-правовими засадами захисту інформації та персональних даних;
- формування навичок розпізнавання соціальної інженерії, фішингу, інтернет-шахрайства та інших загроз цифрового середовища;
- опанування принципів і практичних засобів ідентифікації, автентифікації, авторизації та управління доступом до інформаційних ресурсів;
- набуття практичних умінь щодо захисту електронних документів, хмарних сховищ, цифрових сервісів та освітніх інформаційних систем;
- формування навичок організації резервного копіювання, відновлення даних і безпечного передавання інформації комп’ютерними мережами;
- ознайомлення з методами фізичного захисту інформації та запобігання її витоку технічними каналами;
- розвиток умінь розробляти базові політики інформаційної безпеки, здійснювати моніторинг стану захищеності інформаційних ресурсів і визначати порядок реагування на інформаційні інциденти;
- формування відповідального ставлення до захисту інформації, дотримання цифрової етики та правил безпечної професійної діяльності.

**2. Компетентності**

**СК05** — Здатність використовувати сучасні інформаційні технології та спеціалізоване програмне забезпечення та інтегрувати їх в освітнє середовище.

**СК08** — Здатність використовувати відповідне програмне забезпечення для вирішення професійних завдань, відповідно до спеціалізації.

**СК09** — Здатність здійснювати професійну діяльність з дотриманням вимог законодавства, стандартів освіти та внутрішніх нормативних документів закладу освіти.

**СК14** — Здатність збирати, аналізувати та інтерпретувати інформацію (дані) відповідно до

спеціалізації.

**СК16** — Здатність до системного аналізу технічних і педагогічних систем, процесів та ситуацій, вивчення передового виробничого та педагогічного досвіду, впровадження досягнень вітчизняної й зарубіжної науки і техніки.

**СК24** — Здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення.

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

| № | Назва теми | **Лекції** денна/ заочна | **Практ./ Семін./ лаб** денна/ заочна | **Самост. робота** денна/ заочна | Разом | Методи навчання | Методи оцінювання | СК |
|---|---|---|---|---|---|---|---|---|
| **Змістовий модуль 1. Теоретичні, організаційні та правові основи захисту інформації** | | | | | | | | |
| 1 | Тема 1. Інформація як об’єкт захисту. Основні поняття інформаційної безпеки | 2/2 | 2/0 | 6/8 | 10/10 | МН1, МН2, МН3, МН4, МН6 | МО2, МО4, МО7 | СК14, СК16 |
| 2 | Тема 2. Загрози, вразливості та порушники інформаційної безпеки | 2/0 | 2/0 | 6/10 | 10/10 | МН1, МН2, МН3, МН4, МН6 | МО2, МО4, МО7 | СК14, СК16 |
| 3 | Тема 3. Оцінювання ризиків інформаційної безпеки | 2/0 | 2/0 | 6/10 | 10/10 | МН1, МН2, МН3, МН4, МН6 | МО2, МО4, МО7 | СК14, СК16 |
| 4 | Тема 4. Методи та принципи комплексного захисту інформації | 2/2 | 2/0 | 6/8 | 10/10 | МН1, МН2, МН3, МН4, МН6 | МО2, МО4, МО7 | СК08, СК16, СК24 |
| 5 | Тема 5. Соціальна інженерія та інтернет-шахрайство | 2/0 | 2/0 | 6/10 | 10/10 | МН1, МН2, МН3, МН4, МН5, МН6 | МО2, МО4, МО7 | СК14, СК16 |
| 6 | Тема 6. Правові основи захисту інформації. Персональні дані | 2/0 | 2/0 | 6/10 | 10/10 | МН1, МН2, МН3, МН4, МН6 | МО2, МО4, МО7 | СК09 |
| 7 | Тема 7. Ідентифікація, автентифікація та управління доступом | 2/0 | 2/2 | 6/8 | 10/10 | МН1, МН2, МН3, МН4, МН5, МН6 | МО2, МО4, МО7, Модульна контрольна робота | СК08, СК24 |
| **Змістовий модуль 2. Практичні технології захисту інформації** | | | | | | | | |

| № | Назва теми | **Лекції** денна/ заочна | **Практ./ Семін./ лаб** денна/ заочна | **Самост. робота** денна/ заочна | **Разом** | **Методи навчання** | **Методи оцінювання** | **СК** |
|---|---|---|---|---|---|---|---|---|
| 8 | Тема 8. Захист електронних документів і безпечна спільна робота | 2/0 | 2/0 | 6/10 | 10/10 | МН1, МН2, МН3, МН4, МН5, МН6 | МО2, МО4, МО7 | СК05, СК08, СК09 |
| 9 | Тема 9. Безпека хмарних сховищ та хмарних сервісів | 2/0 | 2/0 | 6/10 | 10/10 | МН1, МН2, МН3, МН4, МН5, МН6 | МО2, МО4, МО7 | СК05, СК08, СК24 |
| 10 | Тема 10. Захист інформації в освітніх платформах і системах дистанційного навчання | 2/0 | 2/0 | 6/10 | 10/10 | МН1, МН2, МН3, МН4, МН5, МН6 | МО2, МО4, МО7 | СК05, СК08, СК09, СК24 |
| 11 | Тема 11. Резервне копіювання та відновлення інформації | 2/0 | 2/2 | 6/8 | 10/10 | МН1, МН2, МН3, МН4, МН5, МН6 | МО2, МО4, МО7 | СК08, СК24 |
| 12 | Тема 12. Захист інформації під час передавання комп’ютерними мережами | 2/2 | 2/0 | 6/8 | 10/10 | МН1, МН2, МН3, МН4, МН5, МН6 | МО2, МО4, МО7 | СК08, СК24 |
| 13 | Тема 13. Фізичний захист інформації та технічні канали її витоку | 2/0 | 2/0 | 6/10 | 10/10 | МН1, МН2, МН3, МН4, МН6 | МО2, МО4, МО7 | СК16 |
| 14 | Тема 14. Політика інформаційної безпеки закладу освіти | 2/0 | 2/0 | 6/10 | 10/10 | МН1, МН2, МН3, МН4, МН6 | МО2, МО4, МО7 | СК05, СК09, СК16 |
| 15 | Тема 15. Моніторинг безпеки та реагування на інформаційні інциденти | 2/0 | 2/2 | 6/8 | 10/10 | МН1, МН2, МН3, МН4, МН5, МН6 | МО2, МО4, МО7, Модульна контрольна робота | СК08, СК14, СК16, СК24 |
| | **Разом** | **30/6** | **30/6** | **90/138** | **150/150** | | | |

*Легенда: 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: МО2 — усне або письмове опитування; МО4 — тестування; МО7 — презентації результатів виконаних завдань та досліджень.*

**4. Результати навчання**

**Знати:**

– основні поняття інформаційної безпеки, властивості конфіденційності, цілісності й доступності інформації та принципи захисту інформаційних активів;

– види загроз і вразливостей, характеристики потенційних порушників та основні підходи до побудови моделі загроз;

– етапи оцінювання й оброблення ризиків інформаційної безпеки, призначення матриці ризиків;

– організаційні, правові, програмні, технічні та фізичні методи комплексного захисту інформації;

– типові прийоми соціальної інженерії, ознаки фішингу та способи протидії інтернет-шахрайству;

– основні нормативно-правові засади захисту інформації й персональних даних, права суб'єктів даних та обов'язки учасників їх оброблення;

– принципи ідентифікації, автентифікації, авторизації та управління доступом, призначення багатофакторної автентифікації й менеджерів паролів;

– способи захисту електронних документів, призначення електронного підпису та правила безпечної спільної роботи;

– загрози безпеці хмарних сервісів і освітніх платформ, принципи розподіленої відповідальності та розмежування прав користувачів;

– види й засоби резервного копіювання, принцип 3-2-1 та основні показники відновлення інформації RPO і RTO;

– принципи захищеного передавання інформації, призначення HTTPS, TLS і VPN та основи безпеки бездротових мереж;

– основні фізичні загрози й технічні канали витоку інформації та способи їх обмеження;

– складові політики інформаційної безпеки закладу освіти, основи моніторингу безпеки й етапи реагування на інформаційні інциденти.

**Вміти:**

– визначати інформаційні активи та вимоги до їх конфіденційності, цілісності й доступності;

– виявляти загрози й вразливості цифрового освітнього середовища, складати базову модель загроз і потенційного порушника;

– оцінювати ймовірність і наслідки реалізації загроз, будувати матрицю ризиків та обґрунтовувати пріоритетні заходи захисту;

– добирати організаційні, програмні, технічні й фізичні засоби захисту відповідно до визначених ризиків;

– розпізнавати ознаки фішингу та соціальної інженерії, перевіряти підозрілі повідомлення, посилання й цифрові ресурси;

– визначати вимоги до оброблення персональних даних у типових професійних ситуаціях і застосовувати принципи мінімізації даних та обмеження доступу;

– налаштовувати надійні паролі, багатофакторну автентифікацію та права доступу користувачів у доступних цифрових сервісах;

– застосовувати засоби захисту електронних документів, налаштовувати дозволи на перегляд,

редагування й поширення та використовувати контроль версій;

– перевіряти й налаштовувати спільний доступ і параметри конфіденційності у хмарних сховищах та освітніх платформах у межах наданих прав;

– розробляти план резервного копіювання, створювати резервні копії та перевіряти можливість відновлення даних;

– перевіряти ознаки захищеного вебз'єднання, добирати безпечні способи передавання даних і налаштовувати базові параметри захисту бездротової мережі в навчальному середовищі;

– аналізувати фізичні загрози робочому місцю й комп'ютерному класу та пропонувати заходи запобігання витоку інформації;

– розробляти базову політику інформаційної безпеки закладу освіти та алгоритм реагування на типовий інцидент, фіксувати його ознаки й визначати порядок повідомлення відповідальних осіб.

**5. Цілі сталого розвитку**

ЦСР 4 – Якісна освіта

ЦСР 9 – Промисловість, інновації та інфраструктура

ЦСР 11 – Сталий розвиток міст і громад

ЦСР 16 – Мир, справедливість та сильні інститути

**6. Неформальна освіта**

Рекомендовано освітній серіал «Персональна кібергігієна» на платформі Дія.Освіта: https://osvita.diia.gov.ua/courses/personal-cyberhygiene. Його матеріали можуть доповнювати опрацювання тем про соціальну інженерію, захист облікових записів, безпеку мереж і фізичний захист інформації.
Результати навчання, здобуті під час тематичних онлайн-курсів, тренінгів та інших заходів неформальної або інформальної освіти, можуть бути визнані відповідно до процедур ЛНТУ за умови їх відповідності результатам навчання дисципліни. Здобувач подає документальне підтвердження, якщо воно передбачене форматом навчання, та опис опанованих тем і досягнутих результатів. За потреби викладач проводить співбесіду або пропонує практичне завдання для перевірки відповідних знань і вмінь. Обсяг і спосіб зарахування визначаються за встановленою в університеті процедурою; наявність сертифіката сама по собі не означає автоматичного зарахування всієї дисципліни.

**7. Критерії та форми контролю**

Оцінювання — за 100-бальною шкалою (національна шкала / ЄКТС). Підсумковий бал = поточний контроль (50 %) + модульний контроль (50 %).

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. Інформація як об'єкт захисту. Основні поняття інформаційної безпеки**

Поняття інформації та її роль у сучасному цифровому суспільстві. Інформація як об'єкт захисту. Види інформації та її класифікація за режимом доступу. Інформаційні ресурси та інформаційні активи. Поняття інформаційної безпеки та захисту інформації. Основні властивості захищеної інформації: конфіденційність, цілісність і доступність. Життєвий цикл інформації та необхідність її захисту на різних етапах. Суб'єкти й об'єкти інформаційної безпеки. Основні принципи забезпечення захисту інформації. Особливості інформаційної безпеки в освітньому та професійному цифровому середовищі.

**Тема 2. Загрози, вразливості та порушники інформаційної безпеки**

Поняття загрози інформаційній безпеці та вразливості інформаційної системи. Класифікація

загроз за джерелами виникнення, характером впливу та об’єктами посягання. Внутрішні й зовнішні загрози. Випадкові та навмисні порушення інформаційної безпеки. Поняття порушника, його можливості, мотиви та цілі. Основні сценарії реалізації загроз. Типові вразливості програмного забезпечення, інформаційних систем і цифрових сервісів. Побудова моделі загроз і моделі потенційного порушника. Аналіз загроз інформаційній інфраструктурі закладу освіти.

**Тема 3. Оцінювання ризиків інформаційної безпеки**

Поняття ризику інформаційної безпеки та його складові. Взаємозв’язок інформаційних активів, загроз, вразливостей і можливих наслідків. Основні етапи управління ризиками. Ідентифікація інформаційних активів та визначення їх критичності. Якісні та кількісні методи оцінювання ризиків. Визначення ймовірності реалізації загроз і рівня потенційних збитків. Матриця ризиків та її практичне застосування. Пріоритезація ризиків. Основні стратегії оброблення ризиків: уникнення, зменшення, передавання та прийняття. Оцінювання ризиків у цифровому освітньому середовищі.

**Тема 4. Методи та принципи комплексного захисту інформації**

Поняття комплексного захисту інформації та його основні завдання. Принципи системності, багаторівневості, мінімальних привілеїв і захисту за замовчуванням. Організаційні, правові, фізичні, технічні та програмні методи захисту інформації. Превентивні, виявлювальні та коригувальні заходи безпеки. Засоби захисту інформаційних ресурсів від несанкціонованого доступу. Призначення антивірусного захисту, міжмережевих екранів та засобів контролю доступу. Основи побудови системи захисту інформації. Поєднання організаційних і технологічних заходів. Оцінювання ефективності засобів захисту інформації.

**Тема 5. Соціальна інженерія та інтернет-шахрайство**

Поняття соціальної інженерії та психологічні механізми маніпулювання користувачами. Основні методи соціальної інженерії: фішинг, цільовий фішинг, вішинг, смішинг, претекстинг і підміна особи. Шахрайські електронні повідомлення, вебсайти та цифрові сервіси. Компрометація облікових записів і викрадення конфіденційної інформації. Шахрайство в соціальних мережах, месенджерах та електронній комерції. Методи перевірки достовірності повідомлень, посилань і цифрових ресурсів. Ознаки підозрілої комунікації. Протидія соціальній інженерії. Формування культури безпечної цифрової поведінки та підвищення обізнаності користувачів.

**Тема 6. Правові основи захисту інформації. Персональні дані**

Нормативно-правове регулювання інформаційних відносин та захисту інформації в Україні. Законодавство у сфері інформації, захисту інформації в інформаційно-комунікаційних системах та захисту персональних даних. Поняття персональних даних, їх категорії та особливості оброблення. Права суб’єктів персональних даних. Обов’язки володільців і розпорядників персональних даних. Правові підстави збирання, зберігання, використання та поширення персональних даних. Принципи мінімізації даних та обмеження доступу. Загальні положення GDPR. Особливості оброблення персональних даних учасників освітнього процесу. Відповідальність за порушення законодавства у сфері захисту інформації.

**Тема 7. Ідентифікація, автентифікація та управління доступом**

Поняття ідентифікації, автентифікації та авторизації користувачів. Основні фактори автентифікації: знання, володіння та біометричні характеристики. Парольна автентифікація та вимоги до надійних паролів. Багатофакторна автентифікація та її практичне застосування. Менеджери паролів і засоби захисту облікових записів. Поняття управління доступом до інформаційних ресурсів. Основні моделі контролю доступу: дискреційна, мандатна, рольова та атрибутивна. Принцип найменших привілеїв. Розмежування прав користувачів у цифрових сервісах, хмарних сховищах та освітніх інформаційних системах. Контроль активних сеансів і запобігання несанкціонованому доступу.

**Тема 8. Захист електронних документів і безпечна спільна робота**

Електронні документи як об’єкти інформаційного захисту. Основні загрози конфіденційності, цілісності та доступності електронних документів. Методи обмеження доступу до файлів і документів. Захист документів паролями та налаштування дозволів на перегляд, редагування й

поширення. Призначення електронного підпису та перевірка цілісності й автентичності електронних документів. Контроль версій і відстеження змін. Організація безпечної спільної роботи з документами в Microsoft 365 і Google Workspace. Ризики використання публічних посилань і спільних папок. Захист конфіденційної інформації під час обміну електронними документами. Особливості захисту навчальної та службової документації.

**Тема 9. Безпека хмарних сховищ та хмарних сервісів**

Поняття хмарних технологій та основні моделі надання хмарних послуг. Особливості зберігання й оброблення інформації у хмарному середовищі. Основні загрози безпеці хмарних сховищ і сервісів. Модель розподіленої відповідальності за інформаційну безпеку між провайдером і користувачем. Захист облікових записів і налаштування параметрів конфіденційності. Управління правами доступу до файлів і папок у Google Drive, OneDrive та інших хмарних сховищах. Контроль спільного доступу та відкликання дозволів. Захист даних під час синхронізації між пристроями. Відновлення видалених файлів і використання історії версій. Оцінювання ризиків використання хмарних сервісів в освітній і професійній діяльності.

**Тема 10. Захист інформації в освітніх платформах і системах дистанційного навчання**

Особливості забезпечення інформаційної безпеки цифрового освітнього середовища. Основні загрози інформаційним ресурсам закладів освіти. Захист персональних даних здобувачів освіти, педагогічних працівників та інших учасників освітнього процесу. Безпека систем управління навчанням Moodle, Google Classroom та інших освітніх платформ. Управління обліковими записами й розмежування прав доступу викладачів, здобувачів освіти та адміністраторів. Захист електронних журналів, результатів оцінювання та навчальних матеріалів. Безпечне проведення відеоконференцій і дистанційних занять. Запобігання несанкціонованому доступу до навчальних курсів і цифрових освітніх ресурсів. Організаційні заходи захисту інформації в освітньому середовищі.

**Тема 11. Резервне копіювання та відновлення інформації**

Поняття резервного копіювання та його значення для забезпечення доступності й цілісності інформації. Основні причини втрати даних. Види резервного копіювання: повне, інкрементне та диференціальне. Локальне, мережеве та хмарне резервне копіювання. Принцип резервування даних 3-2-1 та його практичне застосування. Вибір носіїв і засобів резервного копіювання. Планування періодичності створення резервних копій. Автоматизація резервного копіювання. Захист резервних копій від несанкціонованого доступу, пошкодження та шкідливого програмного забезпечення. Перевірка цілісності резервних копій і тестування відновлення даних. Основні показники відновлення інформації RPO та RTO. Розроблення плану резервного копіювання для особистих і професійних інформаційних ресурсів.

**Тема 12. Захист інформації під час передавання комп’ютерними мережами**

Основні загрози інформації під час передавання комп’ютерними мережами. Перехоплення мережевого трафіку, підміна даних, атаки типу «людина посередині» та несанкціонований доступ. Принципи захищеного передавання інформації. Призначення протоколів HTTPS і TLS. Перевірка захищеності вебз’єднань і цифрових сертифікатів. Поняття віртуальних приватних мереж (VPN) та особливості їх використання. Безпека бездротових мереж Wi-Fi. Протоколи захисту WPA2 і WPA3. Налаштування базових параметрів безпеки домашніх і навчальних мереж. Призначення міжмережевих екранів. Ризики використання відкритих бездротових мереж. Практичні рекомендації щодо безпечного передавання інформації в локальних і глобальних мережах.

**Тема 13. Фізичний захист інформації та технічні канали її витоку**

Поняття фізичного захисту інформації та його місце в системі інформаційної безпеки. Основні фізичні загрози інформаційним ресурсам і технічним засобам. Несанкціонований фізичний доступ до комп’ютерного обладнання, носіїв інформації та мережевої інфраструктури. Організація контролю фізичного доступу до приміщень і обладнання. Засоби відеоспостереження, сигналізації та обліку доступу. Захист інформаційних носіїв під час зберігання, транспортування та утилізації. Поняття технічних каналів витоку інформації. Акустичні, оптичні та електромагнітні канали витоку. Загальні принципи запобігання витоку

інформації технічними каналами. Захист робочих місць і комп’ютерних класів. Забезпечення фізичної безпеки інформаційних ресурсів закладу освіти.

**Тема 14. Політика інформаційної безпеки закладу освіти**

Поняття політики інформаційної безпеки, її призначення та основні складові. Організаційне забезпечення інформаційної безпеки закладу освіти. Розподіл відповідальності за захист інформаційних ресурсів. Основні вимоги до використання комп’ютерного обладнання, мережевих ресурсів, електронної пошти та хмарних сервісів. Правила створення й використання облікових записів. Політика паролів та управління доступом. Вимоги до оброблення й зберігання персональних даних учасників освітнього процесу. Організація резервного копіювання та оновлення програмного забезпечення. Правила використання особистих пристроїв у професійній діяльності. Ознайомлення з основними положеннями міжнародного стандарту ISO/IEC 27001. Розроблення базової політики інформаційної безпеки закладу освіти. Формування культури інформаційної безпеки.

**Тема 15. Моніторинг безпеки та реагування на інформаційні інциденти**

Поняття моніторингу інформаційної безпеки та його основні завдання. Інформаційні події, інциденти та порушення безпеки. Основні ознаки компрометації інформаційних ресурсів і облікових записів. Призначення журналів подій та засобів моніторингу. Виявлення підозрілої активності в інформаційних системах і цифрових сервісах. Основні етапи реагування на інциденти інформаційної безпеки: підготовка, виявлення, аналіз, локалізація, усунення наслідків і відновлення роботи. Документування та повідомлення про інциденти. Дії користувача у випадку втрати пристрою, компрометації облікового запису, витоку персональних даних або зараження шкідливим програмним забезпеченням. Аналіз причин інцидентів і запобігання їх повторенню. Розроблення алгоритмів реагування на типові інциденти інформаційної безпеки в закладі освіти.

## 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. Мельничук Ю. Є. Інтелектуальні технології в освіті : навчальний посібник. Луцьк : Терен, 2023. 241 с.

2. Мельничук Ю. Є. Проектування інформаційних систем : методичні вказівки до лабораторних занять для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності А5.39

«Професійна освіта (Цифрові технології)». Луцьк : ЛНТУ, 2026. 60 с. URL: https://repository.lntu.edu.ua/handle/123456789/3070

*Праці інших авторів:*

3. Pascoe C., Quinn S., Scarfone K. NIST Cybersecurity Framework 2.0: Quick-Start Guide for Creating and Using Organizational Profiles. NIST Special Publication 1301. Gaithersburg : National Institute of Standards and Technology, 2024. DOI: https://doi.org/10.6028/NIST.SP.1301

4. Quinn S., Pascoe C., Barrett M., Scarfone K., Witte G. NIST Cybersecurity Framework 2.0: Quick-Start Guide for Using the CSF Tiers. NIST Special Publication 1302. Gaithersburg : National Institute of Standards and Technology, 2024. DOI: https://doi.org/10.6028/NIST.SP.1302

**ІІ. Наукові праці**

*Праці автора силабуса:*

5. Nadolska V., Melnychuk Y. Information security in higher education institutions of Ukraine: analysis of risks and management strategies. Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate. 2026. Vol. 16, No. 1. P. 65–75. DOI: https://doi.org/10.24917/26578549.16.1.4

6. Мельничук Ю., Полухтович Т. Хмарні технології та онлайн-сервіси: вплив на цифрову трансформацію суспільства. Наукові інновації та передові технології. 2025. № 4(44). С. 1311–1321. DOI: https://doi.org/10.52058/2786-5274-2025-4(44)-1311-1321

7. Мельничук Ю. Є. Принципи побудови інформаційних систем освітнього призначення. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2023. № 50. С. 77–84. DOI: https://doi.org/10.36910/6775-2524-0560-2023-50-11

8. Мельничук Ю. Є. Алгоритми функціонування інформаційних систем освітнього призначення. Наука і техніка сьогодні. 2023. № 3(17). С. 576–585. DOI: https://doi.org/10.52058/2786-6025-2023-3(17)-576-585

*Праці інших авторів:*

9. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Papers. CSWP 29. National Institute of Standards and Technology, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29

10. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST Special Publication 800-61, Revision 3. National Institute of Standards and Technology, 2025. DOI: https://doi.org/10.6028/NIST.SP.800-61r3

11. European Union Agency for Cybersecurity. ENISA Threat Landscape 2025. ENISA, 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

12. European Union Agency for Cybersecurity. ENISA Threat Landscape 2026. ENISA, 2026. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2026

13. European Union Agency for Cybersecurity. ENISA Cybersecurity Threat Landscape Methodology. ENISA, 2025. URL: https://www.enisa.europa.eu/publications/enisa-cybersecurity-threat-landscape-methodology

**ІІІ. Інформаційні ресурси**

14. Законодавство України : офіційний вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/

15. Державна служба спеціального зв’язку та захисту інформації України : офіційний вебсайт. URL: https://cip.gov.ua/

16. CERT-UA — урядова команда реагування на комп’ютерні надзвичайні події України. URL: https://cert.gov.ua/

17. Рада національної безпеки і оборони України : офіційний вебсайт, матеріали Національного координаційного центру кібербезпеки. URL: https://www.rnbo.gov.ua/

18. National Institute of Standards and Technology. Computer Security Resource Center. URL: https://csrc.nist.gov/

19. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/

20. OWASP Foundation. Open Worldwide Application Security Project. URL: https://owasp.org/

21. Cybersecurity and Infrastructure Security Agency (CISA). URL: https://www.cisa.gov/

22. Дія.Освіта : національна освітня платформа актуальних цифрових навичок. URL: https://osvita.diia.gov.ua/

23. Google Safety Center : рекомендації та інструменти цифрової безпеки. URL: https://safety.google/