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 «Оцінка та управління ризиками»
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/2328

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Оцінка та управління ризиками»

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
Викладач(і)	к.т.н., доцент Сергій КОСТЮЧКО

1. Мета і завдання дисципліни

Мета: Знайомство студентів із основними фундаментальними поняттями і законами теорії ризиків для їх використання в сучасних кіберсистемах; принципами побудови алгоритмів оцінки ризиків у кібербезпеці, основних стандартів оцінки ризиків та їх використання в задачах захисту інформації; основним математичним апаратом та законами оцінки ризиків у професійній діяльності; програмними засобами, які реалізують основні алгоритми оцінки ризиків для вирішення типових задач захисту інформації.

Завдання: Завдання дисципліни полягає в поглибленні знань в області безпеки комп’ютерних мереж та систем. Предмет присвячений вивченню та засвоєнню сучасних технологій, які використовуються для організації кібербезпеки.

Пререквізити: Аналіз великих даних, Інформаційна безпека бізнесу

2. Компетентності

СК03 — Здатність до використання програмних та програмно апаратних комплексів засобів захисту інформації в інформаційнотелекомунікаційних (автоматизованих) системах.

СК04 — Здатність забезпечувати неперервність бізнесу згідно встановленої політики 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. Управління кіберінцидентами: Поняття кіберінцидента/кібератаки. Розслідування кіберінцидентів/кібератак.								
1	Тема 1. Поняття кіберінцидента/кібератаки	2/0,5	2/0,5	6/12	10/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК03, СК04
2	Тема 2. Розслідування кіберінцидентів/кібератак	2/0,5	2/0,5	6/12	10/13	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК03, СК04
3	Тема 3. Управління ризиками в інформаційній та/або кібербезпеці	2/0,5	2/0,5	6/14	10/15	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК03, СК04
4	Тема 4. Загальна концепція управління ризиками ІБ	2/0,5	2/0,5	6/16	10/17	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК03, СК04

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
5	Тема 5. NIST SP 800x	6/2	6/2	18/20	30/24	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК03, СК04
6	Тема 6. Системи класу Incident Response Platform	4/0,5	4/0,5	12/16	20/17	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК03, СК04
Змістовий модуль 2. Управління ризиками в інформаційній та/або кібербезпеці								
7	Тема 7. Етапи проведення аудиту. Аудит на основі аналізу ризиків	4/0,5	4/0,5	12/16	20/17	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК03, СК04
8	Тема 8. Аудит на основі стандартів інформаційної безпеки (ІБ). Аудит на основі експертних досліджень інформаційних систем (ІС). Забезпечення безперервності бізнес-процесів: Поняття бізнес- процесу. Модель бізнес-процесу	4/0,5	4/0,5	12/16	20/17	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК03, СК04
9	Тема 9. Розробка політик інформаційної безпеки під час забезпечення бізнес-процесів. Дотримання політик інформаційної безпеки під час забезпечення бізнес-процесів	4/0,5	4/0,5	12/16	20/17	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК03, СК04
	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); 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

ПРН04. аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

ПРН12. розробляти моделі загроз та порушника;

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;

ПРН29. здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;

ПРН30. здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;

ПРН33. вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

ПРН44. вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;

ПРН45. застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

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

5. Цілі сталого розвитку

ЦСР 8 – Гідна праця та економічне зростання

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. Поняття кіберінцидента/кібератаки

Основні поняття кібербезпеки. Визначення кіберінциденту та кібератаки. Види та класифікація кіберінцидентів. Основні типи кібератак та способи їх реалізації. Джерела кіберзагроз. Поняття вразливості, загрози та ризику. Ознаки та індикатори компрометації інформаційних систем. Життєвий цикл кібератаки. Основні принципи виявлення та запобігання кіберінцидентам.

Тема 2. Розслідування кіберінцидентів/кібератак

Поняття та основні завдання розслідування кіберінцидентів. Етапи розслідування кібератак. Виявлення, реєстрація та класифікація інцидентів. Збирання та збереження цифрових доказів. Аналіз журналів подій операційних систем і мережевого обладнання. Аналіз мережевого трафіку. Визначення джерел та причин інцидентів. Основи цифрової криміналістики (Digital Forensics). Документування результатів розслідування. Розроблення рекомендацій щодо запобігання повторним інцидентам.

Тема 3. Управління ризиками в інформаційній та/або кібербезпеці

Поняття ризику інформаційної безпеки. Основні складові ризику. Класифікація ризиків інформаційної та кібербезпеки. Ідентифікація інформаційних активів і загроз. Виявлення вразливостей інформаційних систем. Методи якісного та кількісного оцінювання ризиків. Визначення ймовірності реалізації загроз та можливих наслідків. Матриця ризиків. Пріоритизація ризиків. Основні способи оброблення ризиків. Моніторинг та перегляд ризиків.

Тема 4. Загальна концепція управління ризиками ІБ

Основні принципи та завдання управління ризиками. Життєвий цикл управління ризиками інформаційної безпеки. Визначення контексту та критеріїв ризику. Формування реєстру ризиків. Поняття прийнятного та залишкового ризику. Розроблення плану оброблення ризиків. Вибір організаційних і технічних заходів захисту. Розподіл відповідальності за управління ризиками. Документування та контроль ризиків. Основні положення ISO/IEC 27005 та ISO 31000.

Тема 5. NIST SP 800x

Призначення та структура спеціальних публікацій NIST SP 800. Основні положення NIST SP 800-30 щодо оцінювання ризиків. NIST SP 800-37 та концепція Risk Management Framework (RMF). Каталог заходів безпеки NIST SP 800-53. Управління кіберінцидентами відповідно до NIST SP 800-61. Основи реагування на кіберінциденти. Визначення рівнів ризику та вибір заходів захисту. Практичне застосування рекомендацій NIST для забезпечення кібербезпеки інформаційних систем.

Тема 6. Системи класу Incident Response Platform

Поняття та призначення платформ реагування на інциденти інформаційної безпеки. Основні функції Incident Response Platform (IRP). Реєстрація, класифікація та пріоритизація інцидентів. Управління життєвим циклом інцидентів. Інтеграція IRP із системами SIEM, EDR та засобами моніторингу. Автоматизація процесів реагування. Поняття SOAR (Security Orchestration, Automation and Response). Використання TheHive та аналогічних платформ. Формування сценаріїв реагування (Playbooks). Документування та аналіз результатів реагування на інциденти.

Тема 7. Етапи проведення аудиту. Аудит на основі аналізу ризиків

Поняття та призначення аудиту інформаційної безпеки. Основні цілі та завдання аудиту. Види аудиту інформаційних систем. Планування та підготовка аудиту. Визначення об'єктів і критеріїв аудиту. Збирання та аналіз аудиторських доказів. Оцінювання ризиків інформаційної безпеки. Визначення критичних інформаційних активів. Виявлення недоліків системи захисту. Формування аудиторського звіту. Розроблення рекомендацій щодо зменшення ризиків.

Тема 8. Аудит на основі стандартів інформаційної безпеки (ІБ). Аудит на основі експертних досліджень інформаційних систем (ІС). Забезпечення безперервності бізнес-процесів: Поняття бізнес- процесу. Модель бізнес-процесу

Поняття стандартизованого аудиту інформаційної безпеки. Міжнародні та національні стандарти у сфері захисту інформації. Основні положення ISO/IEC 27001 та ISO/IEC 27002. Рекомендації ISO/IEC 27007 щодо аудиту систем управління інформаційною безпекою. Використання NIST Cybersecurity Framework. Перевірка відповідності політик і процедур вимогам стандартів. Формування контрольних списків аудиту. Аналіз невідповідностей. Документування результатів перевірки. Підготовка рекомендацій щодо вдосконалення системи інформаційної безпеки.

Тема 9. Розробка політик інформаційної безпеки під час забезпечення бізнес-процесів. Дотримання політик інформаційної безпеки під час забезпечення бізнес-процесів

Поняття та призначення політики інформаційної безпеки. Основні принципи розроблення політик безпеки. Структура та зміст політики інформаційної безпеки організації. Визначення вимог до захисту інформаційних активів. Розроблення політик управління доступом, резервного копіювання, використання інформаційних ресурсів та реагування на інциденти. Врахування ризиків і критичності бізнес-процесів. Розподіл ролей та відповідальності. Погодження, затвердження та впровадження політик. Періодичний перегляд та актуалізація документів з інформаційної безпеки.

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. 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. 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 Rev. 3. Gaithersburg : National Institute of Standards and Technology, 2025. URL: https://doi.org/10.6028/NIST.SP.800-61r3.

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

14. National Institute of Standards and Technology. NIST Cybersecurity Framework 2.0 : Resource and Overview Guide : NIST Special Publication 1299. Gaithersburg : NIST, 2024. URL: https://doi.org/10.6028/NIST.SP.1299.

15. ISO/IEC 27006-1:2024. Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General. Geneva : International Organization for Standardization, 2024. 47 p. URL: https://www.iso.org/standard/82908.html.

16. ISO 22301:2019/Amd 1:2024. Security and resilience — Business continuity management systems — Requirements — Amendment 1: Climate action changes. Geneva : International Organization for Standardization, 2024. URL: https://www.iso.org/standard/88412.html.