**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 «Системи моніторингу комп'ютерних систем та мереж»**
**ступінь вищої освіти – бакалавр**
**галузь знань – 12 Інформаційні технології**
**спеціальність – 125 Кібербезпека та захист інформації**
**освітня програма – Кібербезпека**

**Кафедра кібербезпеки**

Силабус склав(ла) асистент (ПП) кафедри кібербезпеки Роман ВОЗНЮК

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/2310

**Луцьк – 2026**

**СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Системи моніторингу комп'ютерних систем та мереж»**

| | |
|---|---|
| **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** | 6 кредитів ECTS / 180 годин, семестр 5 |
| **Форма контролю** | екзамен |
| **Викладач(і)** | асистент (пп) Роман ВОЗНЮК |

**1. Мета і завдання дисципліни**

**Мета:** Забезпечення знань основ аналізу журналів і метрик, розслідування інцидентів в інфраструктурі.

**Завдання:** надання студентам знань з принципів збору і обробки журналів систем та їх метрик, які їм необхідні в практичній діяльності;
знати наявні рішення в сегменті систем моніторингу, прийоми, методи, базові знання з роботи в стекові ELK (Elastic, Logstash, Kibana);
вміти розгорнути стек на потрібній кількості серверів, організувати збір журналів і метрик з цільових пристроїв, розробити шаблони і фільтри для обробки полів журналів, аналізувати отриману інформацію, розслідувати базові інциденти.

**Пререквізити:** Комп'ютерні мережі, Захист операційних систем, Безпека інформаційно-комунікаційних систем

**2. Компетентності**

**ІК — інтегральна компетентність:** Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

**ЗК01** — Здатність застосовувати знання у практичних ситуаціях.

**ЗК04** — Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

**СК02** — Здатність до використання інформаційно комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

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

**СК11** — Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

**СК12** — Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою 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 |
|---|---|---|---|---|---|---|---|---|

| № | Назва теми | Лекції денна/ заочна | Лаб. денна/ заочна | Самост. робота денна/ заочна | Разом | Методи навчання | Методи оцінювання | ЗК та СК |
|---|---|---|---|---|---|---|---|---|
| **Змістовий модуль 1. Вступ до моніторингу** | | | | | | | | |
| 1 | Тема 1. Вступ до моніторингу: цілі та завдання | 2/0,5 | 4/0,5 | 5/10 | 11/11 | МН1, МН2, МН3, МН4, МН5 | МО1, МО2, МО4, МО5 | ЗК01, ЗК04, СК02, СК12 |
| 2 | Тема 2. Архітектура систем моніторингу | 2/0,5 | 2/0,5 | 5/15 | 9/16 | МН1, МН2, МН3, МН4, МН5 | МО1, МО2, МО4, МО5 | ЗК01, ЗК04, СК02, СК03, СК11, СК12 |
| 3 | Тема 3. Створення моніторингового середовища | 2/0,5 | 4/1 | 10/15 | 16/16,5 | МН1, МН2, МН3, МН4, МН5 | МО1, МО2, МО4, МО5 | ЗК01, ЗК04, СК02, СК03, СК11, СК12 |
| 4 | Тема 4. Сучасні системи моніторингу | 4/0,5 | 7/1 | 10/20 | 21/21,5 | МН1, МН2, МН3, МН4, МН5 | МО1, МО2, МО4, МО5 | ЗК01, ЗК04, СК02, СК03, СК11, СК12 |
| 5 | Тема 5. Метрики та логи, методи їх збору (SNMP, WMI, API) | 2/– | 2/0,5 | 10/15 | 14/15,5 | МН1, МН2, МН3, МН4, МН5 | МО1, МО2, МО4, МО5 | ЗК01, ЗК04, СК02, СК03, СК11, СК12 |
| **Змістовий модуль 2. Аналітика і візуалізація моніторингу** | | | | | | | | |
| 6 | Тема 6. Аналітика і візуалізація моніторингу | 2/0,5 | 4/1 | 10/15 | 16/16,5 | МН1, МН2, МН3, МН4, МН5 | МО1, МО2, МО4, МО5 | ЗК01, ЗК04, СК02, СК03, СК11, СК12 |
| 7 | Тема 7. Моніторинг інформаційно – комунікаційної інфраструктури | 2/0,5 | 4/1 | 10/15 | 16/16,5 | МН1, МН2, МН3, МН4, МН5 | МО1, МО2, МО4, МО5 | ЗК01, ЗК04, СК02, СК03, СК11, СК12 |
| 8 | Тема 8. Моніторинг мережевого обладнання | 2/0,5 | 4/1 | 10/10 | 16/11,5 | МН1, МН2, МН3, МН4, МН5 | МО1, МО2, МО4, МО5 | ЗК01, ЗК04, СК02, СК03, СК11, СК12 |
| 9 | Тема 9. Моніторинг серверів та віртуальних середовищ | 2/0,5 | 4/1 | 10/10 | 16/11,5 | МН1, МН2, МН3, МН4, МН5 | МО1, МО2, МО4, МО5 | ЗК01, ЗК04, СК02, СК03, СК11, СК12 |

| № | Назва теми | Лекції денна/ заочна | Лаб. денна/ заочна | Самост. робота денна/ заочна | Разом | Методи навчання | Методи оцінювання | ЗК та СК |
|---|---|---|---|---|---|---|---|---|
| 10 | Тема 10. Системи і протоколи централізованого логування: Syslog, Graylog | 2/– | 4/1 | 10/10 | 16/11 | МН1, МН2, МН3, МН4, МН5 | МО1, МО2, МО4, МО5 | ЗК01, ЗК04, СК02, СК03, СК11, СК12 |
| 11 | Тема 11. Тригери, сповіщення та реагування на інциденти | 2/– | 2/0,5 | 5/10 | 9/10,5 | МН1, МН2, МН3, МН4, МН5 | МО1, МО2, МО4, МО5 | ЗК01, ЗК04, СК02, СК03, СК11, СК12 |
| 12 | Тема 12. Моніторинг безпеки: IDS/IPS, SIEM, SOC практики | 2/– | 2/0,5 | 5/10 | 9/10,5 | МН1, МН2, МН3, МН4, МН5 | МО1, МО2, МО4, МО5 | ЗК01, ЗК04, СК02, СК03, СК11, СК12 |
| 13 | Тема 13. Нормативна база моніторингу та реагування на кіберінциденти | 4/– | 2/0,5 | 5/11 | 11/11,5 | МН1, МН2, МН3, МН4, МН5 | МО1, МО2, МО4, МО5 | ЗК01, ЗК04, СК02, СК12 |
| | **Разом** | **30/4** | **45/10** | **105/166** | **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.*

## 4. Результати навчання

**ПРН05.** адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

**ПРН11.** виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;

**ПРН15.** використовувати сучасне програмно-апаратне забезпечення інформаційнокомунікаційних технологій;

**ПРН20.** забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

**ПРН25.** забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;

**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;

**ПРН41.** забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

**ПРН48.** виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційнотелекомунікаційних системах;

**ПРН49.** забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;

**ПРН52.** використовувати інструментарій для моніторингу процесів в інформаційнотелекомунікаційних системах;

## 5. Цілі сталого розвитку

ЦСР 9 – Промисловість, інновації та інфраструктура

ЦСР 11 – Сталий розвиток міст і громад

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. Вступ до моніторингу: цілі та завдання

Складання карти цілей моніторингу університетської мережі.
Визначення критичних сервісів університетської мережі, що потребують моніторингу.
Порівняльний аналіз реактивного та проактивного підходів до моніторингу мережі.

### Тема 2. Архітектура систем моніторингу

Розроблення схеми архітектури системи моніторингу та порівняльний аналіз централізованої і децентралізованої архітектур.

### Тема 3. Створення моніторингового середовища

Встановлення та налаштування середовища віртуалізації Proxmox Virtual Environment (PVE).
Інсталяція та налаштування віртуальних операційних систем Windows і Linux.
Налаштування мережевого середовища для функціонування систем моніторингу.

### Тема 4. Сучасні системи моніторингу

Встановлення та налаштування системи моніторингу PRTG.
Встановлення та налаштування системи моніторингу Zabbix.
Встановлення та налаштування системи моніторингу Nagios.
Розгортання та налаштування Elasticsearch для збирання й аналізу даних моніторингу.
Налаштування протоколів і розгортання агентів збирання даних та порівняльний аналіз систем моніторингу.

### Тема 5. Метрики та логи, методи їх збору (SNMP, WMI, API)

Налаштування збирання метрик із використанням SNMP, WMI та API.

**Тема 6. Аналітика і візуалізація моніторингу**

Створення інформаційної панелі (дашборду) в Grafana на основі даних систем моніторингу.
Побудова порівняльних графіків показників моніторингу за тижневий період.

**Тема 7. Моніторинг інформаційно – комунікаційної інфраструктури**

Налаштування моніторингу доступності ключових мережевих сервісів.
Визначення критичних вузлів інформаційно-комунікаційної інфраструктури, проведення навантажувального тестування та аналіз отриманих результатів.

**Тема 8. Моніторинг мережевого обладнання**

Збирання статистичних даних мережевих інтерфейсів комутатора з використанням протоколу SNMP.
Побудова графіків використання пропускної здатності мережевих інтерфейсів.

**Тема 9. Моніторинг серверів та віртуальних середовищ**

Налаштування моніторингу завантаження процесора (CPU), оперативної пам'яті (RAM) та дискової підсистеми (Disk).
Моніторинг стану віртуальних машин у середовищах VMware та Proxmox.

**Тема 10. Системи і протоколи централізованого логування: Syslog, Graylog**

Розгортання системи Graylog та налаштування підключення джерел журналів подій.
Налаштування передавання та централізованого збирання журналів подій за протоколом Syslog.

**Тема 11. Тригери, сповіщення та реагування на інциденти**

Створення та налаштування тригерів для виявлення втрати з'єднання на мережевому комутаторі.
Налаштування тригерів контролю перевищення встановлених порогів використання дискового простору в середовищах VMware та Proxmox.

**Тема 12. Моніторинг безпеки: IDS/IPS, SIEM, SOC практики**

Встановлення та базове налаштування системи управління інформацією та подіями безпеки (SIEM).
Аналіз інцидентів інформаційної безпеки з використанням системи SIEM.

**Тема 13. Нормативна база моніторингу та реагування на кіберінциденти**

Ознайомлення з основними положеннями Закону України «Про основні засади забезпечення кібербезпеки України».

## 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**

**II. Наукові праці**

*Праці інших авторів:*

1. Голубничий Д. Ю., Коцюба В. П. Застосування технологій моніторингу та аналізу стану IP-мережі на основі використання протоколу SNMP. Вісник Харківського національного автомобільно-дорожнього університету. Харків, 2022. Вип. 96. С. 14–21. URL: http://nbuv.gov.ua/UJRN/vhad_2022_96_4.

2. Коваленко О. Є., Кузнюк К. В. Системи моніторингу комп'ютерних мереж. Математичні машини і системи. 2023. № 1. С. 50–59. URL: http://www.immsp.kiev.ua/publications/articles/2023/2023_1/01_23_Kovalenko.pdf.

3. Cyber Security Training, Certifications & Research. SANS Institute. URL: https://www.sans.org/emea/.

**III. Інформаційні ресурси**

4. Threat Hunting with Elastic Stack. O’Reilly Online Learning. URL: https://www.oreilly.com/library/view/threat-hunting-with/9781801073783/.

5. Офіційна документація Elasticsearch. Elastic. URL: https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html.

6. Офіційна документація Kibana. Elastic. URL: https://www.elastic.co/guide/en/kibana/current/index.html.

7. Офіційна документація Logstash. Elastic. URL: https://www.elastic.co/guide/en/logstash/current/index.html.

8. Quickly Get Started with Elastic. Elastic. URL: https://www.elastic.co/getting-started#quick-starts.

9. Zabbix: The Enterprise-Class Open Source Network Monitoring Solution. Zabbix. URL: https://www.zabbix.com/.

10. Splunk: The Key to Enterprise Resilience. Splunk. URL: https://www.splunk.com/.

11. Wazuh – Open Source XDR, Open Source SIEM. Wazuh. URL: https://wazuh.com/.

12. Prometheus – Monitoring System & Time Series Database. Prometheus. URL: https://prometheus.io/.

13. Graylog. URL: https://graylog.org/.

14. Nagios Open Source. Nagios. URL: https://www.nagios.org/.