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 «Обробка інцидентів та реагування»
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 Олег КУЛАКЕВИЧ

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/2932

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Обробка інцидентів та реагування»

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 6
Форма контролю	екзамен
Викладач(і)	асистент (пп) Олег КУЛАКЕВИЧ

1. Мета і завдання дисципліни

Мета: Метою вивчення навчальної дисципліни «Обробка інцидентів та реагування» є формування у здобувачів вищої освіти системних теоретичних знань і практичних навичок щодо виявлення, аналізу, класифікації та обробки інцидентів кібербезпеки, а також організації ефективного реагування на них. Особлива увага приділяється опануванню сучасних методів, технологій та інструментальних засобів моніторингу інформаційних систем, встановлення причин виникнення інцидентів, локалізації загроз, усунення їх наслідків і відновлення нормального функціонування інформаційної інфраструктури з метою забезпечення її конфіденційності, цілісності та доступності.

Завдання: Основними завданнями навчальної дисципліни є формування знань щодо принципів організації процесів управління інцидентами кібербезпеки, набуття практичних навичок виявлення, реєстрації, класифікації та аналізу інцидентів, опанування методів оцінювання їх критичності та потенційних наслідків. У межах дисципліни передбачається вивчення сучасних технологій моніторингу та аналізу подій безпеки, процедур локалізації й усунення кіберзагроз, методів цифрової криміналістики, документування результатів розслідування, а також розроблення заходів щодо відновлення працездатності інформаційних систем і запобігання повторному виникненню інцидентів.

Пререквізити: Програмування та реверс-інжиніринг, Комп'ютерні мережі, Захист операційних систем, Системи моніторингу комп'ютерних систем та мереж

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.

ЗК05 — Здатність до пошуку, оброблення та аналізу інформації.

СК04 — Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

СК08 — Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

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.								
1	Тема 1. Вступ до обробки інцидентів та реагування	2/0,5	2/0,75	7/11,25	11/12,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК04, СК08
2	Тема 2. Різновиди інцидентів в інформаційних системах	2/0,5	2/0,75	7/11,25	11/12,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК04, СК08
3	Тема 3. Методи виявлення інцидентів	2/0,5	2/0,5	7/11,25	11/12,25	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК04, СК08
4	Тема 4. Моніторинг та логування в інформаційних системах	2/0,5	2/0,5	7/11,25	11/12,25	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК04, СК08
5	Тема 5. Аналіз наслідків інцидентів та розробка стратегій реагування	2/0,5	2/0,5	7/11	11/12	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК04, СК08
6	Тема 6. Комунікація під час реагування на інциденти	2/0,5	2/0,5	7/11	11/12	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК04, СК08
7	Тема 7. Управління інцидентами та системи управління інцидентами	2/0,5	2/0,5	7/11	11/12	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК04, СК08
8	Тема 8. Командний підхід до реагування на інциденти	2/0,5	3/0,5	7/11	12/12	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК05, ЗК04, СК04, СК08
Змістовий модуль 2.								
9	Тема 9. Стандарти та нормативно-правові акти в галузі обробки інцидентів	2/0,5	4/0,5	7/11	13/12	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК04, СК08

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
10	Тема 10. Інциденти безпеки інформації та кібербезпека	2/0,25	4/0,5	7/11	13/11,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК04, СК08
11	Тема 11. Відновлення після інциденту та планування заходів у разі виникнення інцидентів	2/0,25	4/0,5	7/11	13/11,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК04, СК08
12	Тема 12. Робота з внутрішніми та зовнішніми стейкхолдерами під час реагування на інциденти	2/0,25	4/0,5	7/11	13/11,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК08, СК04
13	Тема 13. Аудит та оцінка ефективності системи реагування на інциденти	2/0,25	4/0,5	7/11	13/11,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК04, СК08
14	Тема 14. Використання інструментів для збору, аналізу та візуалізації даних відносно інцидентів	2/0,25	4/0,5	7/11	13/11,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК04, СК08
15	Тема 15. Порівняння різних підходів до реагування на інциденти в різних сферах діяльності	2/0,25	4/0,5	7/11	13/11,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	ЗК01, ЗК04, ЗК05, СК04, СК08
	Разом	**30/6**	**45/8**	**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

ПРН30. здійснювати оцінювання можливості несанкціонованого доступу до елементів

інформаційно-телекомунікаційних систем;

ПРН32. вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

ПРН34. приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

ПРН50. забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);

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 обробки інцидентів та реагування

Поняття та сутність інцидентів інформаційної безпеки. Основні цілі та завдання реагування на інциденти. Життєвий цикл управління інцидентами кібербезпеки. Основні етапи виявлення, аналізу, локалізації та усунення інцидентів. Роль реагування на інциденти в системі забезпечення кібербезпеки організації.

Тема 2. Різновиди інцидентів в інформаційних системах

Класифікація інцидентів інформаційної безпеки. Інциденти, пов'язані з несанкціонованим доступом, шкідливим програмним забезпеченням та витоком інформації. Мережеві атаки, фішинг, атаки типу DoS/DDoS. Внутрішні та зовнішні загрози. Визначення критичності інцидентів та оцінювання їх впливу на інформаційні системи.

Тема 3. Методи виявлення інцидентів

Основні підходи до виявлення інцидентів кібербезпеки. Сигнатурні, аномальні та поведінкові методи виявлення загроз. Використання систем IDS/IPS, EDR та SIEM. Аналіз мережевого трафіку та подій безпеки. Застосування машинного навчання для виявлення підозрілої активності.

Тема 4. Моніторинг та логування в інформаційних системах

Призначення та організація моніторингу інформаційної інфраструктури. Джерела подій безпеки та типи журналів реєстрації. Централізований збір, зберігання й обробка логів. Кореляція подій та виявлення аномалій. Використання інструментів моніторингу та аналізу журналів безпеки.

Тема 5. Аналіз наслідків інцидентів та розробка стратегій реагування

Методи оцінювання масштабів і наслідків інцидентів кібербезпеки. Аналіз впливу інцидентів на конфіденційність, цілісність і доступність інформації. Визначення пріоритетів реагування. Розроблення стратегій локалізації, стримування та усунення загроз. Оцінювання ризиків і вибір оптимальних заходів реагування.

Тема 6. Комунікація під час реагування на інциденти

Організація інформаційної взаємодії під час реагування на інциденти. Внутрішні та зовнішні канали комунікації. Порядок повідомлення про інциденти та ескалації подій. Документування процесу реагування. Забезпечення конфіденційності інформації під час комунікації.

Тема 7. Управління інцидентами та системи управління інцидентами

Принципи побудови процесів управління інцидентами. Організація реєстрації, класифікації та супроводу інцидентів. Системи обліку й управління інцидентами. Автоматизація процесів реагування з використанням SOAR-платформ. Інтеграція засобів моніторингу, аналізу та управління інцидентами.

Тема 8. Командний підхід до реагування на інциденти

Організаційна структура команд реагування на інциденти кібербезпеки. Функції та завдання SOC, CSIRT і CERT. Розподіл ролей і відповідальності між учасниками команди. Координація дій під час розслідування та ліквідації інцидентів. Організація командних навчань і моделювання кіберінцидентів.

Тема 9. Стандарти та нормативно-правові акти в галузі обробки інцидентів

Міжнародні стандарти та рекомендації щодо управління інцидентами інформаційної безпеки. Вимоги ISO/IEC 27035 та рекомендації NIST щодо реагування на інциденти. Нормативно-правове регулювання кібербезпеки в Україні. Вимоги до повідомлення про кіберінциденти та їх документування. Відповідність процедур реагування нормативним вимогам.

Тема 10. Інциденти безпеки інформації та кібербезпека

Взаємозв'язок інформаційної безпеки та кібербезпеки. Основні джерела кіберзагроз і вразливості інформаційних систем. Типові сценарії реалізації кіберінцидентів. Методи аналізу кіберзагроз та індикаторів компрометації (IoC). Використання MITRE ATT&CK для дослідження тактик і технік зловмисників.

Тема 11. Відновлення після інциденту та планування заходів у разі виникнення інцидентів

Основні етапи відновлення інформаційних систем після інцидентів. Розроблення планів реагування та відновлення після кіберінцидентів. Резервне копіювання та відновлення даних. Забезпечення безперервності бізнес-процесів і відновлення працездатності критичних сервісів. Аналіз причин інцидентів та формування коригувальних і превентивних заходів.

Тема 12. Робота з внутрішніми та зовнішніми стейкхолдерами під час реагування на інциденти

Визначення зацікавлених сторін у процесі реагування на інциденти. Організація взаємодії між технічними підрозділами, керівництвом та користувачами інформаційних систем. Співпраця з національними командами реагування, правоохоронними органами та зовнішніми експертами. Порядок обміну інформацією про інциденти. Координація спільних заходів із локалізації та усунення кіберзагроз.

Тема 13. Аудит та оцінка ефективності системи реагування на інциденти

Мета та завдання аудиту процесів реагування на інциденти. Методи оцінювання ефективності систем виявлення та реагування. Ключові показники ефективності реагування (MTTD, MTTR). Аналіз відповідності процедур реагування встановленим політикам і стандартам. Розроблення рекомендацій щодо вдосконалення системи управління інцидентами.

Тема 14. Використання інструментів для збору, аналізу та візуалізації даних відносно інцидентів

Програмні засоби збору та обробки інформації про події безпеки. Використання SIEM-платформ для аналізу інцидентів. Інструменти аналізу мережевого трафіку та системних журналів.

Візуалізація подій безпеки за допомогою інформаційних панелей. Побудова звітів, графіків і часових діаграм інцидентів. Автоматизація аналізу та формування сповіщень про загрози.

Тема 15. Порівняння різних підходів до реагування на інциденти в різних сферах діяльності

Особливості організації реагування на кіберінциденти в державних установах, фінансових організаціях, медичних закладах та промислових підприємствах. Порівняння централізованих і децентралізованих моделей реагування. Особливості реагування на інциденти в хмарних, корпоративних та промислових інформаційних системах. Аналіз практичних сценаріїв кіберінцидентів. Визначення критеріїв вибору ефективних стратегій реагування відповідно до специфіки діяльності організації.

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

ІІ. Наукові праці

Праці інших авторів:

1. Digital Forensics and Incident Response. 3rd ed. O’Reilly Online Learning. URL: https://www.oreilly.com/library/view/digital-forensics-and/9781803238678/.

2. Monitoring Network Devices with Wazuh. Wazuh. URL: https://wazuh.com/blog/monitoring-network-devices/.

3. Anson S., Bunting S., Pearson S. Mastering Windows Network Forensics and Investigation. Scribd. URL: https://www.scribd.com/book/101821418/Mastering-Windows-Network-Forensics-and-Investigation.

4. NIST SP 800-61. NIST. URL: https://www.nist.gov/privacy-framework/nist-sp-800-61.

5. Simplify Security Complexity with Cybersecurity for Automotive. SystemWeaver. URL: https://systemweaver.com/in-use/cybersecurity.

6. National Institute of Standards and Technology. NIST. URL: https://www.nist.gov/.

7. SP 800-61 Rev. 2. Computer Security Incident Handling Guide. NIST Computer Security Resource Center (CSRC). URL: https://csrc.nist.gov/pubs/sp/800/61/r2/final.

8. CERT-UA. cert.gov.ua. URL: https://cert.gov.ua/.

9. ДСТУ ISO/IEC 27035-1:2018. Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами (ISO/IEC 27035-1:2016, IDT). БУДСТАНДАРТ Online. URL:

https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80309.

10. ДСТУ ISO/IEC 27035-2:2018. Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2016, IDT). БУДСТАНДАРТ Online. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80310.

11. ISO/IEC 27000. International Organization for Standardization. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27000:ed-5:v1:en.

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

13. Collaboration Software for Software, IT and Business Teams. Atlassian. URL: https://www.atlassian.com/.

14. Velocidex/velociraptor: Digging Deeper. GitHub. URL: https://github.com/Velocidex/velociraptor.

15. eHealth Україна. Вебінар 8 «План та порядок реагування на інциденти інформаційної безпеки». 2023. YouTube. URL: https://www.youtube.com/watch?v=TUKFMSutVq4.