МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативного освітнього компонента
Комплексна система захисту інформації
першого (бакалаврського) рівня
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми
Кібербезпека та захист інформації

Луцьк – 2025

Силабус освітнього компонента «Комплексні системи захисту інформації» підготовки для першого (бакалаврського) рівня вищої освіти галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації.

Розробники:
доцент, кандидат технічних наук Онищук Оксана Олександрівна

Погоджено

Гарант освітньо-професійної програми:  Чернящук Н.Л.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 2 від 17 вересня 2025 р.

Завідувач кафедри:  Гришанович Т. О.

1.Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність,

освітня програма,</th><th>Характеристика освітнього компонента</th></tr>
<tr><td>Денна форма навчання</td><td rowspan="6">12 Інформаційні технології
125 Кібербезпека та захист інформації
Кібербезпека та захист інформації бакалавр</td><td>Нормативна</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів 150/5</td><td>Рік навчання 4</td></tr>
<tr><td>Семестр_8-ий</td></tr>
<tr><td>Лекцій: 56 год.</td></tr>
<tr><td>Лабораторні роботи : 70 год.</td></tr>
<tr><td>ІНДЗ: немає</td><td>Самостійна робота 14 год.</td></tr>
<tr><td></td><td>Консультації: 10 год.</td></tr>
<tr><td></td><td>Форма контролю: екзамен</td></tr>
<tr><td colspan="3">Мова навчання: українська</td></tr>
</table>

ІІ. Інформація про викладача

ПІП – Онищук Оксана Олександрівна
Науковий ступінь – кандидат технічних наук
Вчене звання – доцент
Посада – доцент комп'ютерних наук та кібербезпеки
Контактна інформація: +38-0966943585, Onyshchuk.oksana@vnu.edu.ua

ІІІ. Опис дисципліни

1. Анотація курсу. Освітній компонент «Комплексні системи захисту інформації» відноситься до переліку дисциплін циклу професійної підготовки. Освітній компонент присвячений підвищенню рівня знань здобувачів з теорії і практики захисту інформації технічними засобами, набуття вмінь і навичок з виявлення технічних каналів витоку інформації, їх блокування, створенні та впровадженні комплексів технічного захисту інформації, в знанні основ організації та порядку виконання робіт із створення комплексних систем захисту інформації телекомунікаційних систем залежно від характеру об’єкта захисту.

2. Мета і завдання освітнього компонента: метою «Комплексні системи захисту інформації» є вироблення у здобувачів теоретичних знань та практичних навичок самостійної роботи з забезпечення комплексного захисту інформації на об’єктах інформаційної діяльності на основі нормативно-правових документів, національних та міжнародних стандартів. Дати здобувачам поглиблені знання в опануванні загальних теоретичних знань та практичних навичок щодо розробки типової стратегії і організації комплексної системи захисту інформації. Вивчення особливостей побудови комплексних систем захисту інформації та централізованого управління системою інформаційної безпеки.

3.Результати навчання.

Загальні компетентності:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні) компетентності

СК 1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК4. Здатність забезпечувати захист інформації інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)

СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.

СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об’єктах інформаційної діяльності.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків.

РН 5. 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.

РН 7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

РН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

РН 20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

4. Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам. роб.	Конс.	Форма контролю/ Бали
Змістовий модуль 1. Нормативно-правові акти комплексної системи захисту інформації.						
Тема 1. Загальні положення та вимоги в частині організації робіт із захисту інформації.	11	4	5	1	1	Звіт по лаб. роботі/5
Тема 2. Правові підстави та основні положення щодо створення КСЗІ та комплексу ТЗІ в Україні	11	4	5	1	1	Звіт по лаб. роботі/5
Тема 3. Основні положення про службу захисту інформації. Технічний захист інформації.	11	4	5	1	1	Звіт по лаб. роботі/5
Тема 4. Захист інформації в АС від НСД.	11	4	5	1	1	Звіт по лаб. роботі/5
Тема 5.Захист інформації в АС від витоку технічними каналами	11	4	5	1	1	Звіт по лаб. роботі/5
Тема 6. Захист інформації в АС від руйнування каналами спеціального впливу.	10	4	5	1		Звіт по лаб. роботі /5
Тема 7. Порядок проведення робіт зі створення КСЗІ.	10	4	5	1		Звіт по лаб. роботі /5
Разом за модулем 1	75	28	35	7	5	35
Змістовий модуль 2. Побудова системи і основних підсистем КСЗІ						
Тема 1. Технічне завдання на створення КСЗІ в АС.	13	5	6	2		Звіт по лаб. роботі/6

Тема 2. Основи захисту інформації в ІС.	13	5	6	1	1	Звіт по лаб. роботі/ 6
Тема 3. Особливості проектування КСЗІ для АС різних класів. Оцінка ефективності та оптимізація КСЗІ.	13	5	6	1	1	Звіт по лаб. роботі /6
Тема 4. Перспективні напрями розвитку комплексу ЗІ в розподілених обчислювальних середовищах (РОС).	13	5	6	1	1	Звіт по лаб. роботі/6
Тема 5. Випробування комплексу технічного захисту інформації та його атестація.	12	4	6	1	1	Звіт по лаб. роботі/6
Тема 6. Введення КСЗІ в дію.	11	4	5	1	1	Звіт по лаб. роботі/5
Разом за модулем 2	75	28	35	7	5	35
Модульна контрольна робота 1						15
Модульна контрольна робота 2						15
ІНДЗ						
Всього годин/Балів	150	56	70	14	10	100

Методи контролю*: ДС – дискусія, ДБ – дебати, Т – тести, ТР – тренінг, РЗ/К – розв'язування задач/кейсів, ІНДЗ/ІРС – індивідуальне завдання/індивідуальна робота здобувача освіти, РМГ – робота в малих групах, МКР/КР – модульна контрольна робота/ контрольна робота, Р – реферат, а також аналітична записка, аналітичне есе, аналіз твору тощо.

5. Завдання для самостійного опрацювання.

Самостійна робота здобувачів включає в себе: опрацювання лекційного матеріалу (перевірка здійснюється під час лабораторних занять та оцінюється при виставленні оцінки за змістовий модуль); підготовка до лабораторних занять, виконання домашніх завдань (перевірка здійснюється під час лабораторних занять); систематизація вивченого матеріалу перед контрольними заходами, тестуванням (перевірка здійснюється під час контрольних заходів, тестування); вивчення тем, що не розглядаються в курсі лекцій (перевірка здійснюється під час модульних контрольних заходів і оцінюється відповідною кількістю балів).

№ з/п	Тема	Кількість годин
1	Правові підстави та основні положення щодо створення КСЗІ та комплексу ТЗІ в Україні	2
2	Основні положення про службу захисту інформації. Технічний захист інформації.	2
3	Захист інформації в АС від НСД.	2

4	Захист інформації в АС від руйнування каналами спеціального впливу.	2
5	Основи захисту інформації в ІС.	1
6	Перспективні напрями розвитку комплексу ЗІ в розподілених обчислювальних середовищах (РОС).	1
7	Випробування комплексу технічного захисту інформації та його атестація	1
8	Особливості проектування КСЗІ для АС різних класів. Оцінка ефективності та оптимізація КСЗІ.	1
9	Технічне завдання на створення КСЗІ в АС	1
	Всього	14

IV. Політика оцінювання Політика викладача щодо студента

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загальноприйнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття; списування. Очікується, що всі студенти відвідають усі лекції і лабораторні заняття курсу. Завдання для практичного виконання (лабораторні роботи, ІНДЗ, самостійні роботи), завдання підсумкового контролю (тести, контрольні роботи, що передбачають розробку програм) здаються із використанням засобів дистанційного курсу.

Під час вивчення освітнього компонента можливе визнання інших результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті. Порядок визнання результатів навчання для здобувачів вищої освіти, набутих у: формальній освіті (академічна мобільність студентів на території України чи поза її межами, для студентів, які переводяться, поновлюються з інших ЗВО (вітчизняних чи іноземних); неформальній та/або інформальній освіті здійснюється згідно «ПОЛОЖЕННЯ про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки».

Політика щодо академічної доброчесності

Під час навчання учасники освітнього процесу зобов’язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності.

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі

використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання студенти не користуються забороненими засобами (мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси), самостійно виконують запропоновані завдання. При виконанні лабораторних робіт з курсу здобувачі мають право використовувати власні ноутбуки, якщо вони підтримують необхідне програмне забезпечення.

Політика щодо дедлайнів та перескладання

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона вивчають теоретичний матеріал самостійно використовуючи навчальні посібники, конспекти лекцій, матеріали дистанційного курсу "Комплексна система захисту інформації", розміщених на платформі дистанційного навчання Moodle, виконують всі домашні завдання. Прозвітуватися про виконання завдань можна, використовуючи вищезазначені дистанційні курси, або під час консультацій, одночасно при цьому з'ясувати незрозумілі моменти, задати питання викладачу. Існує можливість використання форуму дистанційного курсу. Перескладання контрольних робіт та тестувань заборонено.

V. Підсумковий контроль

Підсумковою формою контролю освітнього компонента "Комплексна система захисту інформації" є іспит.

Оцінювання навчальних досягнень здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах, вчасне і якісне виконання домашніх завдань) та підсумковий контроль (самостійне виконання індивідуальних завдань, контрольні роботи, перевірка теоретичної підготовки у формі тестування, ІНДЗ). Максимальна кількість балів, яку може отримати здобувач під час поточного оцінювання за семестр – 70 балів. Максимальна кількість балів, яку може отримати здобувач за підсумковий контроль за семестр складає 30 балів.

Якщо за результатами семестру накопичено не менше 75 балів і студент погоджується із цим результатом, то оцінка за семестр може виставлятися без складання іспиту. В іншому випадку студент складає іспит; максимальна кількість балів, яку можна отримати на іспиті – 60 балів. Вони замінюють бали модульного семестрового контролю, поточний семестровий контроль при цьому зберігається.

Іспит передбачає виконання тестових завдань (10 питань по одному балу) та відповідь на питання (30 балів) Викладач залишає за собою право ставити уточнюючі питання під час відповіді студента та просити прокоментувати програмний код. Студент повинен використати засобі тієї мови програмування, яка вказана у завданні.

Питання для іспиту

1. Назвіть методи підвищення енергетичної та структурної таємності системи передавання інформації.

2. Дайте визначення поняття комплексного захисту інформації

3. Які вам відомі підходи до класифікації загроз безпеці інформації?

4. Порівняйте їх між собою з огляду найбільшої відповідності практичним потребам створення систем захисту інформації.

5. Охарактеризуйте основні принципи системної класифікації загроз безпеці інформації.

6. Наведіть кваліфікаційну структуру каналів несанкціонованого отримання інформації.

7. Дайте класифікацію джерел витоку інформації.

8. Розкрийте зміст методів контролю інформації технічними засобами в каналах телефонного зв'язку.

9. Назвіть методи контролю інформації, що обробляється засобами обчислювальної техніки.

10. Охарактеризуйте основні способи запобігання витоку інформації по технічних каналах. Охарактеризуйте способи захисту інформації в каналах зв'язку.

11. Сформулюйте основні концептуальні положення теорії захисту інформації.

12. Розкрийте зміст функції захисту інформації. Які з функцій утворюють повну множину функцій захисту?

13. Сформулюйте завдання захисту і назвіть десять класів завдань, що створюють репрезентативну множину задач захисту.

14. Приведіть класифікацію засобів захисту інформації. Які переваги і недоліки програмних, апаратних та організаційних засобів захисту інформації?

15. Як впливають показники інформації, що захищається, на структуру і
підходи до проектування системи захисту інформації?

16. Розкрийте зміст короткострокового, середньострокового і довгострокового управління процесами захисту інформації.

17. Сформулюйте основні вимоги до системи нормативно-правових документів, що регламентують процеси комплексного захисту інформації.

18. Сформулювати задачу оптимального вибору методів захисту для кожного конкретного об’єкта і для системи в цілому.

19. Розкрити критерій вибору засобів і методів захисту.

20. Розкрити задачу мінімізації вартості та ефективності забезпечення систем захисту об’єкта.

21. Розкрити задачу мінімізації вірогідності злому усіх методів, які використовуються для захисту об’єкта.

22. Розкрити задачу мінімізації втрат від злому усіх механізмів захисту (методів захисту), які використовуються для захисту об’єкта.

23. Розкрити та пояснити заходи, які виконуються при створенні КСЗІ.

24. Програмні закладки та їх складові. Класифікація програмних закладок.

25. Які основні характеристики телекомунікаційної системи як об'єкта захисту.

26.Розкрийте поняття загрози інформаційної безпеки. Які основні напрями захисту інформації?

27.Класифікація загроз інформаційної безпеки за компонентами інформаційних систем, на які вони націлені.

28.Класифікація загроз інформаційної безпеки за характером впливу

29.Класифікація загроз інформаційної безпеки за розміщенням їх джерела. Які основні види загроз безпеки інформаційним технологіям?

30.Основні техногенні передбачувані та непередбачені загрози інформаційній системи

31.Яку систему складають дестабілізуючі чинники відповідно до технології і функціонування інформації?

32.Привести структуру каналу витоку інформації та дати характеристику середовищу передачі інформації.

33.Які основні методи захисту від витоку інформації з обмеженим доступом шляхом прослуховування?

34.Як залежно від типу створюваного електромагнітного поля розрізняють види екранування?

35.Які методи забезпечують зниження потужності випромінювань і наведень?

36.Які основні методи захисту інформації від НСД в автоматизованих системах?

37.Дайте характеристику основним та допоміжним технічним засобам та системам.

38.Розкрийте поняття зони 1, зони 2 та контрольованої зони.

39.Умови обробки інформації в системі.

40.Критерії оцінки захищеності інформації в АС від НСД. КВ-4.

41.Яка інформація в захищеній системі підлягає обов'язковій реєстрації.

42.Критерії оцінки захищеності інформації в АС від НСД. ЦД-1.

43.Що таке АС класу «1», «2», «3».

44.Критерії оцінки захищеності інформації в АС від НСД. ЦД-2.

45.Порядок розроблення та оформлення програм і методик випробувань Що наводять у розділі “Вимоги щодо забезпечення охорони державної таємниці».

46.Критерії оцінки захищеності інформації в АС від НСД. ЦД-3.

47.Атестація комплексів ТЗІ.

48.Основні етапи атестації комплексу ТЗІ.

49.Критерії оцінки захищеності інформації в АС від НСД. ЦД-4.

50.Зміст другого етапу створення комплексу ТЗІ “Розроблення та впровадження заходів із захисту інформації” на ОІД.

51.Завдання Служби захисту інформації.

VI. Шкала оцінювання

Шкала оцінювання знань здобувачів освіти з освітніх компонентів, де формою контролю є іспит

Оцінка в балах	**Лінгвістична оцінка**	**Оцінка за шкалою ECTS**	
		оцінка	**пояснення**

90–100	Відмінно	A	відмінне виконання
82–89	Дуже добре	B	вище середнього рівня
75–81	Добре	C	загалом хороша робота
67–74	Задовільно	D	непогано
60–66	Достатньо	E	виконання відповідає мінімальним критеріям
1–59	Незадовільно	Fx	необхідне перескладання

VI. Рекомендована література та інтернет-ресурси

Основна література:

1. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 с.
2. A.O. Korchenko, V.O. Breslavskyi, S.P Yevseiev, N.K. Zhumangalieva, A.O. Zvarych, S.V. Kazmirchuk, O.A. Kurchenko, O.A. Laptiev, O. V. Severinov, S. S. Tkachuk. Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. Eastern-European journal of enterprise technologies. Vol.1№2 (109), 2021 pp. 14–23. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2021.225346.
3. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615.
4. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., & others. (2021). *Synergy of building cybersecurity systems*. Kharkiv: PC Technology Center. https://repository.hneu.edu.ua/jspui/bitstream/123456789/25623/1/Монографія%20ІТОГ.pdf https://doi.org/10.21303/2461-4262.2021.001615
5. Korchenko, A. O., Breslavskyi, V. O., Yevseiev, S. P., Zhumangalieva, N. K., Zvarych, A. O., Kazmirchuk, S. V., Kurchenko, O. A., Laptiev, O. A., Severinov, O. V., & Tkachuk, S. S. (2021). Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. *Eastern-European Journal of Enterprise Technologies*, *1*(2(109)), 14–23. https://doi.org/10.15587/1729-4061.2021.225346
6. Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., & Manzhul, I. (2021). Modeling the protection of personal data from trust and the amount of information on social networks. *EUREKA: Physics and Engineering*, *1*, 24–31. https://doi.org/10.21303/2461-4262.2021.001615

Додаткова література:

1. Yevseiev, S., Laptiev, O., Milov, O., & Breslavskyi, V. (2022). Development of a method for checking vulnerabilities of a corporate network using Bernstein transformations. *Eastern-European Journal of Enterprise Technologies, 3*(2(117)), 45–56. https://doi.org/10.15587/1729-4061.2022.253530

2. Li, H., Zhang, Y., & Wang, T. (2025). Advancing cybersecurity with honeypots and deception. *Information, 12*(1), 14. https://www.mdpi.com/2227-9709/12/1/14

3. Tseng, C.-L., & Chang, P.-C. (2024). Developing high-interaction honeypots to capture and analyze region-specific bot behaviors. *HoTSoS 2024 Proceedings*. Johns Hopkins University. https://isi.jhu.edu/wp-content/uploads/2024/02/Honeypot_Paper_for_HoTSoS-2024-2.pdf

4. Kuhrer, M., & Holz, T. (2021). Gotta catch 'em all: A multistage framework for honeypot fingerprinting. *arXiv preprint arXiv:2109.10652*. https://arxiv.org/abs/2109.10652

5. Chothia, T., & Novakovic, C. (2020). Primer — A tool for testing honeypot measures of effectiveness. *arXiv preprint arXiv:2011.00582*. https://arxiv.org/abs/2011.00582

6. Al-Azizi, A., & Al-Harby, F. (2023). Machine learning approaches for anomaly detection in hybrid cybersecurity architectures. *Computers & Security, 129*, 103175. https://doi.org/10.1016/j.cose.2023.103175

7. Nair, R., & Shukla, R. (2024). AI-driven intrusion detection systems in zero-trust environments. *IEEE Access, 12*, 8795–8810. https://doi.org/10.1109/ACCESS.2024.3357923

8. Patel, K., & Thakur, R. (2022). Blockchain-based models for secure data exchange in cyber-physical systems. *Journal of Information Security and Applications, 68*, 103255. https://doi.org/10.1016/j.jisa.2022.103255

9. Alsmadi, I., & Zarour, M. (2020). A comprehensive study on the role of deception technologies in modern cybersecurity. *Future Internet, 12*(10), 169. https://doi.org/10.3390/fi12100169