МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет економіки та управління
Кафедра економіки і торгівлі

СИЛАБУС
вибіркового освітнього компонента

КІБЕРБЕЗПЕКА У ПІДПРИЄМНИЦТВІ ТА ТОРГІВЛІ

підготовки *магістра*
галузі знань *D Бізнес, адміністрування та право*
спеціальності *D7 Торгівля*
освітньо-професійної програми *Підприємництво, торгівля та організація бізнесу*

Луцьк – 2025

Силабус вибіркового освітнього компонента КІБЕРБЕЗПЕКА У ПІДПРИЄМНИЦТВІ ТА ТОРГІВЛІ підготовки магістра, галузі знань D Бізнес, адміністрування та право, спеціальності D7 Торгівля, за освітньо-професійною програмою Підприємництво, торгівля та організація бізнесу.

Розробник: Шостак Л.В., доцент кафедри економіки і торгівлі, кандидат економічних наук, доцент

Погоджено:
Гарант ОП Підприємництво, торгівля та організація бізнесу  Людмила ШОСТАК

Силабус освітнього компонента затверджено на засіданні кафедри економіки і торгівлі
протокол № 1 від 29.08. 2025 р.

Завідувач кафедри  Олена ПАВЛОВА

І. ОПИС ОСВІТНЬОГО КОМПОНЕНТА

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика освітнього компонента</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="8">D Бізнес, адміністрування та право
D 7 Торгівля Підприємництво, торгівля та організація бізнесу
Другий (магістерський) рівень</td><td>Вибірковий</td></tr>
<tr><td>Рік навчання 2 (2026/2027 н.р.)</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів
120/4</td><td>Семестр 3</td></tr>
<tr><td>Лекції 10 год.</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Практичні 14 год.</td></tr>
<tr><td>Самостійна робота 88 год.</td></tr>
<tr><td>Консультації 8 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
<tr><td colspan="2">Мова навчання</td><td>українська</td></tr>
</table>

ІІ. ІНФОРМАЦІЯ ПРО ВИКЛАДАЧА

ПІБ: Шостак Людмила Василівна
Науковий ступінь: кандидат економічних наук
Вчене звання: доцент
Посада: доцент кафедри економіки і торгівлі
Мобільний телефон: 0503784882
Електронна пошта: **Shostak.Lyudmyla@vnu.edu.ua**
Електронний розклад: http://94.130.69.82/cgi-bin/timetable.cgi?n=700

ІІІ. ОПИС ОСВІТНЬОГО КОМПОНЕНТА

1. Анотація освітнього компонента. Зростання обсягів електронної комерції та цифровізації бізнес-процесів супроводжується збільшенням кіберзагроз. Безпека даних, захист інформаційних систем і протидія шахрайству є ключовими умовами стабільності та довіри до бізнесу. Компонент спрямований на формування знань у сфері кібербезпеки, управління ризиками та впровадження захисних технологій у бізнесі.

2. Мета і завдання освітнього компонента. Метою освітнього компоненту є сформувати компетентності у сфері кібербезпеки підприємництва. **Завдання освітнього компоненту:** ознайомлення з видами кіберзагроз; вивчення механізмів захисту даних; аналіз правових аспектів кібербезпеки; розвиток навичок управління ризиками; формування практичних знань із кіберзахисту бізнесу.

3. Soft skills. Освоєння освітнього компонента спрятиме отриманню таких Soft skills як аналітичне мислення (здатність аналізувати кіберзагрози, оцінювати рівень ризиків, виявляти вразливості у цифрових системах та приймати обґрунтовані рішення для їх усунення); стратегічне планування (уміння розробляти довгострокові стратегії інформаційної безпеки підприємства, будувати системи захисту даних та планувати інцидент-менеджмент); уважність до деталей (здатність ретельно перевіряти налаштування, політики та протоколи безпеки, вчасно виявляти потенційні помилки чи загрози); кризовий менеджмент (уміння діяти швидко та ефективно у випадку кіберінцидентів, координувати команду та мінімізувати наслідки кібератак); відповідальність (усвідомлення важливості захисту даних та конфіденційної

інформації, дотримання стандартів і правових норм кіберзахисту для забезпечення довіри клієнтів та партнерів).

4.Структура освітнього компонента.

Назви змістових модулів і тем	**Усього**	**Лек.**	**Практ.**	**Сам. роб.**	**Конс.**	***Форма контролю/ Бал**
Змістовний модуль 1. Основи кібербезпеки						
Тема 1. Поняття та види кіберзагроз.	18	1	2	14	1	О, Т, СР / 12 балів
Тема 2. Правове регулювання кібербезпеки.	18	1	2	14	1	РЗ/К, О, Т / 12 балів
Тема 3. Технології захисту даних у бізнесі.	19	2	2	14	1	РЗ/К, О, Т, РМГ / 12 балів
Разом за модулем 1	55	4	6	42	3	36 балів
Змістовний модуль 2. Кібербезпека у підприємництві та торгівлі						
Тема 4. Ризики e-commerce та способи їх мінімізації.	21	2	2	15	2	РЗ/К, О, Т, СР / 14 балів
Тема 5. Управління кіберінцидентами.	23	2	4	15	2	РЗ/К, О, Т, РМГ / 15 балів
Тема 6. Кіберстійкість бізнесу.	20	2	2	15	1	РЗ/К, Т, РМГ, СР / 15 балів
Разом за модулем 2	64	6	8	45	5	44 бали
Підсумкова контрольна робота						ПКР / 20 балів
Всього годин / Балів	**120**	**10**	**14**	**88**	**8**	**max 100 балів**

Форма контролю: О – опитування, РЗ/К - розв'язування практичних завдань, кейсів, Т – тести, РМГ -робота в малих групах, СР – самостійна робота здобувача, РМГ – робота в малих групах, ПКР – підсумкова контрольна робота.*

5.Завдання для самостійного опрацювання.

Самостійна робота – це форма організації навчального процесу, за якої заплановані завдання виконуються здобувачами освіти самостійно під методичним керівництвом викладача.

До завдань самостійної роботи, які запропоновані здобувачам освіти, віднесено:

1. Вивчення лекційного матеріалу.
2. Робота з рекомендованою літературою.
3. Підготовка до практичних занять, роботи в малих групах, тестування.
4. Контрольна перевірка знань за запитаннями для самоконтролю.

IV. ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо відвідувань занять: відвідування занять є обов'язковим. Здобувачі освіти зобов'язані дотримуватися термінів, визначених для виконання усіх видів робіт, передбачених силабусом. Пропущені заняття відпрацьовувати у визначений час згідно затвердженого графіка.

За об'єктивних причин (наприклад, хвороба, міжнародне стажування, участь в наукових заходах тощо) навчання може відбуватись в цей період в онлайн формі або за індивідуальним планом за погодженням із викладачем.

Здобувач освіти повинен старанно виконувати завдання, брати активну участь в освітньому процесі.

Політика щодо зарахування результатів формальної, неформальної та інформальної освіти визначається Положенням про визнання результатів, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки (http://surl.li/qbxvmw).

Політика щодо академічної доброчесності окреслюється Положенням про систему запобігання та виявлення академічного плагіату в науковій та навчальній діяльності здобувачів вищої освіти, докторантів, науково-педагогічних і наукових працівників Волинського національного університету імені Лесі Українки (http://surl.li/jntduw) та Кодексом академічної доброчесності Волинського національного університету імені Лесі Українки (http://surl.li/aagxg).

Політика щодо дедлайнів та перескладання: у випадку, якщо здобувач освіти не відвідував окремі аудиторні заняття (з поважних причин), на консультаціях він має право відпрацювати пропущені заняття та добрати ту кількість балів, яку було визначено на пропущені теми.

Політика щодо додаткових (бонусних) балів: здобувачам освіти можуть бути присуджено додаткові (бонусні) бали, які зараховуються як результати поточного контролю максимум 15 балів за такі види робіт: опубліковану наукову статтю у фахових виданнях України чи рецензованих закордонних журналах – 10 балів; публікацію тез – з виступом на конференції 5 балів, без виступу – 3 бали; підготовку та участь у всеукраїнському етапі предметних олімпіад, всеукраїнському та міжнародних конкурсах студентських наукових робіт – 7 балів; перемогу у всеукраїнському етапі предметних олімпіад, всеукраїнському та міжнародних конкурсах студентських наукових робіт – 15 балів; подачу проектних заявок на участь в студентських програмах обміну, стипендійних програмах, літніх та зимових школах тощо – 7 балів.

V. ПІДСУМКОВИЙ КОНТРОЛЬ

Порядок організації поточного та підсумкового контролю знань здобувачів освіти регламентується Положенням про поточне та підсумкове оцінювання знань здобувачів вищої освіти Волинського національного університету імені Лесі Українки від 26.06.2025 р. (https://surli.cc/fgmabz).

Семестровий залік виставляється здобувачам освіти на підставі результатів виконання усіх видів запланованої навчальної роботи протягом семестру за 100-бальною шкалою. У дату складання заліку викладач записує у відомість суму поточних балів, які здобувач освіти набрав під час поточної роботи (шкала від 0 до 100 балів).

У випадку, якщо здобувач освіти протягом поточної роботи набрав менше як 60 балів, він складає залік під час ліквідації академічної заборгованості. У цьому випадку бали, набрані під час поточного оцінювання, анулюються.

Перездача підсумкового контролю освітнього компонента проводиться у вигляді письмової відповіді на одне теоретичне питання (30 балів) та розв’язку двох ситуаційних вправ – по 35 балів кожне). Максимальна оцінка за залік – 100 балів.

Терміни проведення підсумкового семестрового контролю встановлюються графіком освітнього процесу.

Перелік питань на залік

1. Що таке кібербезпека та чому вона важлива для бізнесу?
2. Дайте визначення поняттю «кіберзагроза».
3. Класифікація кіберзагроз: які основні групи виділяють?
4. Що таке вірус та чим він відрізняється від троянської програми?

5. Що таке фішинг та як його розпізнати?
6. Які основні ознаки соціальної інженерії в кібербезпеці?
7. Що таке DoS- та DDoS-атаки?
8. Як працюють шкідливі програми (malware) та які їх види?
9. Які ризики пов’язані з використанням публічних Wi-Fi мереж у бізнесі?
10. Поясніть поняття «інсайдерська загроза».
11. Що таке ransomware та як воно діє?
12. Які основні причини зростання кіберзлочинності?
13. Як кіберзагрози впливають на діяльність підприємства?
14. Що таке атакувальна поверхня (attack surface) у кібербезпеці?
15. Наведіть приклади реальних кіберінцидентів у сфері торгівлі.
16. Основні міжнародні нормативи у сфері кібербезпеки.
17. Які українські закони регулюють кібербезпеку бізнесу?
18. Що таке GDPR і як він впливає на бізнес?
19. Які обов’язки компанії щодо збереження персональних даних?
20. Поясніть принцип «privacy by design».
21. Які вимоги кіберзахисту містить Закон України «Про захист інформації»?
22. Роль міжнародних організацій у сфері кіберзахисту.
23. Що таке ISO/IEC 27001 та його значення для бізнесу?
24. Як здійснюється правове регулювання електронної комерції?
25. Що таке кіберзлочин за міжнародним законодавством?
26. Поясніть, що таке «комплаєнс» у сфері кібербезпеки.
27. Що передбачає Конвенція про кіберзлочинність (Будапештська конвенція)?
28. Як регламентуються питання захисту електронних платежів?
29. Які штрафи передбачені за витік персональних даних?
30. Які вимоги законодавства до зберігання та обробки комерційної інформації?
31. Що таке шифрування даних та його роль у кібербезпеці?
32. Поясніть принципи багатофакторної автентифікації (MFA).
33. Що таке firewall та як він працює?
34. Роль антивірусного програмного забезпечення в бізнесі.
35. Що таке VPN та для чого він використовується?
36. Поясніть принципи резервного копіювання даних.
37. Що таке IDS та IPS системи?
38. Як працює SIEM-система та для чого вона потрібна?
39. Роль систем управління доступом (Access Control).
40. Що таке токенізація даних і де вона застосовується?
41. Як правильно обирати паролі та керувати ними?
42. Що таке Zero Trust Architecture?
43. Як працює технологія блокчейн для захисту транзакцій?
44. Що таке Cloud Security та її ключові принципи?
45. Роль кібергігієни у захисті корпоративних даних.
46. Основні кіберзагрози для e-commerce.
47. Що таке «атака на ланцюг постачання» (Supply Chain Attack)?
48. Як захистити дані користувачів у веб-магазині?
49. Ризики для бізнесу, пов’язані з використанням мобільних додатків.
50. Як уникнути фішингових атак у сфері електронної торгівлі?
51. Що таке шкідливі скрипти Magecart і як вони діють?
52. Роль SSL/TLS сертифікатів у захисті даних клієнтів.
53. Що таке PCI DSS та чому воно важливе для e-commerce?

54. Які є методи захисту платежів онлайн?
55. Поясніть, що таке «тестування на проникнення» (penetration testing).
56. Як забезпечити безпеку даних клієнтів у CRM-системі?
57. Що таке атака типу «людина посередині» (MITM)?
58. Як запобігти витоку даних при хмарному зберіганні?
59. Що таке ботнет і чим він загрожує бізнесу?
60. Як кіберзагрози впливають на репутацію бренду?
61. Що таке кіберінцидент і як його визначити?
62. Етапи реагування на кіберінциденти.
63. Як правильно документувати кіберінциденти?
64. Роль команди CSIRT у компанії.
65. Як створити ефективний план реагування на інциденти (IRP)?
66. Що таке SOC (Security Operations Center)?
67. Які інструменти моніторингу безпеки використовуються у бізнесі?
68. Що таке threat intelligence?
69. Як проводиться розслідування кіберінцидентів?
70. Які основні кроки при інциденті витоку даних?
71. Роль автоматизації у реагуванні на кіберінциденти.
72. Що таке журналювання та логування в кібербезпеці?
73. Як будувати взаємодію з правоохоронними органами при кіберінцидентах?
74. Як правильно інформувати клієнтів про інциденти без втрати довіри?
75. Поясніть різницю між проактивним та реактивним підходом до безпеки.
76. Що таке кіберстійкість і чим вона відрізняється від кібербезпеки
77. Як оцінити рівень кіберстійкості підприємства?
78. Роль резервного копіювання у кіберстійкості бізнесу.
79. Як кіберстійкість впливає на безперервність бізнес-процесів?
80. Що таке disaster recovery plan (DRP)?
81. Як кіберстрахування допомагає бізнесу?
82. Що таке business continuity plan (BCP)?
83. Як мінімізувати людський фактор у кіберризиках?
84. Які навчальні програми підвищують кіберстійкість персоналу?
85. Як побудувати корпоративну політику безпеки?
86. Роль топ-менеджменту у забезпеченні кіберстійкості.
87. Які інвестиції у безпеку найефективніші для бізнесу?
88. Поясніть концепцію «Defense in Depth».
89. Що таке Red Team/Blue Team тренування?
90. Як побудувати стратегію кіберстійкості для стартапів?
91. Чому важливо регулярно оновлювати політики безпеки?
92. Що таке оцінка ризиків (Risk Assessment)?
93. Які стандарти кібербезпеки варто впроваджувати бізнесу?
94. Як використовувати кібераналітику для прогнозування загроз?
95. Чим кіберстійкість відрізняється у малому та великому бізнесі?
96. Які інструменти допомагають прогнозувати кіберзагрози?
97. Як побудувати ефективну систему кіберзахисту для e-commerce?
98. Поясніть роль кіберкультури в організації.
99. Як тренінги з безпеки підвищують кіберстійкість персоналу?
100. Які сучасні технології є трендами у сфері кібербезпеки?

VI. ШКАЛА ОЦІНЮВАННЯ

Оцінювання результатів складання підсумкового контролю у вигляді заліку здійснюється у порядку, передбаченому прийнятою в Університеті системою контролю знань за 100-бальною шкалою з переведенням у лінгвістичну оцінку.

Оцінка в балах	Лінгвістична оцінка
90 – 100	Зараховано
82 – 89	
75 - 81	
67 -74	
60 - 66	
1 – 59	Незараховано (необхідне перескладання)

Критерії оцінювання результатів навчання:

60-100 балів (зараховано): здобувач володіє понятійним і фактичним апаратом освітнього компонента в обсязі, необхідному для подальшого навчання і майбутньої роботи за фахом, здатний виконувати завдання, передбачені силабусом, ознайомлений з основною рекомендованою літературою; при виконанні завдань припускається помилок, але демонструє спроможність їх усувати.

1-59 балів (незараховано): здобувач володіє понятійним і фактичним апаратом освітнього компонента на елементарному рівні, теоретичний зміст курсу не освоєний, необхідні практичні навички роботи не сформовані, більшість передбачених силабусом завдань не виконано або містять грубі помилки.

VII. РЕКОМЕНДОВАНА ЛІТЕРАТУРА ТА ІНТЕРНЕТ-РЕСУРСИ

Основна література

1. Кібербезпека та ризики цифрової трансформації компаній. URL: https://jurkniga.ua/contents/kiberbezpeka-ta-riziki-tsifrovoi-transformatsii-kompaniy.pdf?srsltid=AfmBOoqDJB5tYNqteT4HqEU4wtUznkbc57697unO5ChSHxOtM2rHfdQ1
2. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – Київ: Видавництво НА СБ України, 2020. 256 с.
3. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. Київ.: Видавництво Ліра-К, 2020. 554 с.

Додаткова література

1. Дослідження проблеми кібербезпеки бізнесу в умовах воєнних дій в Україні. URL: https://cybersec.net.ua/statti/762-doslidzhennia-problemy-kiberbezpeky-biznesu-v-umovakh-voiennykh-dii-v-ukraini.html
2. Дубина М., Заєць О. Забезпечення кібербезпеки підприємств електронної комерції в умовах становлення цифрової економіки. *Науковий вісник Полісся*. 2024, № 1 (28). С. 208-223. DOI: https://doi.org/10.25140/2410-9576-2024-1(28)-208-223
3. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, проф. В. Б. Толубка. Київ: ДУТ, 2015. 288 с.
4. Кібербезпека підприємств малого бізнесу на основі рішень та рекомендацій NIST. URL: https://archive.interconf.center/index.php/conference-proceeding/article/view/4231/4268
5. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна

наукова установа «Інститут інформації, безпеки і права НАПрН України»; Нац. бібліотека України ім. В.І.Вернадського. Київ. 2023.№9 . 351 с.

6. Кузьменко О., Маклюк О., Чернишова О. КІБЕРБЕЗПЕКА БІЗНЕСУ ПІД ЧАС ВІЙНИ. *Економіка та суспільство*. 2022, № 44. DOI : https://doi.org/10.32782/2524-0072/2022-44-21

7. Муравський Володимир. Облік та кібербезпека : монографія. Тернопіль : ЗУНУ. 2023. 200 с

8. Огляд ринку кібербезпеки в Україні. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf

9. Шостак Л., Федонюк А., Помазун О. Інформаційно-цифрова безпека електронної торгівлі. *Цифрова економіка та економічна безпека*. 2025, Вип. 2 (17), С. 219-223. DOI : https://doi.org/10.32782/dees.17-36

1. Шостак, Л., Федонюк, А., Помазун, О. Кібербезпека в системі формування бізнес-моделі підприємства в умовах цифрової економіки. *Економіка та суспільство*. 2024, № 64. DOI: https://doi.org/10.32782/2524-0072/2024-64-37

2. Шостак Л., Федонюк А., Помазун О. Особливості кібербезпеки бізнесу в умовах воєнного часу. *Цифрова економіка та економічна безпека*, 2024, №3 (12), С. 121-125. DOI : https://doi.org/10.32782/dees.12-22

3. Шостак Л. В., Помазун О. О. Інформаційна безпека в контексті інноваційного розвитку бізнес-моделі вітчизняних підприємств в умовах цифрової економіки. *Цифрова економіка та економічна безпека.* 2024. URL: http://dees.iei.od.ua/index.php/journal/article/view/464

Інтернет-ресурси

1. Нормативно-правова база України URL: http://zakon3.rada.gov.ua/
2. Кібербезпека підприємства роздрібної торгівлі. URL: https://wiseit.com.ua/fortinet-for-retail/
3. Кібербезпека підприємства. URL: https://yur-gazeta.com/dumka-eksperta/kiberbezpeka-pidpriemstva.html
4. Як підвищити кібербезпеку бізнесу: 10 порад. URL: https://netwave.ua/blog/kiberbezpeka-biznesu/