МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет іноземної філології
Кафедра прикладної лінгвістики

СИЛАБУС

вибіркового освітнього компонента

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

підготовки бакалавра

Луцьк 2025

Силабус освітнього компонента «Основи інформаційної безпеки» підготовки бакалавра.

Розробник:
Крестьянполь Л. Ю., кандидат технічних наук, доцент кафедри прикладної лінгвістики.

Погоджено
Гарант освітньо-професійної програми І.М. Калиновська

Силабус освітнього компонента затверджено на засіданні кафедри прикладної лінгвістики
протокол № 1 від 29.08.2025 р.

В.о. завідувача кафедри І.М. Калиновська

I. Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітня програма, освітній рівень</th><th colspan="3">Характеристика освітнього компонента</th></tr>
<tr><td>Денна / заочна форма здобуття освіти</td><td rowspan="9">В Культура, мистецтво та гуманітарні науки

В11 Філологія

Прикладна лінгвістика. Переклад і комп’ютерна лінгвістика

Бакалавр</td><td colspan="3">Вибірковий</td></tr>
<tr><td rowspan="3">Кількість годин / кредитів 5/150</td><td colspan="3">Рік навчання 4</td></tr>
<tr><td colspan="3">Семестр 7-ий</td></tr>
<tr><td>Форми навчання</td><td>Д</td><td>З</td></tr>
<tr><td rowspan="3">ІНДЗ: є / немає</td><td>Лекції</td><td>10</td><td>4</td></tr>
<tr><td>Практичні (семінарські)</td><td>20</td><td>6</td></tr>
<tr><td>Самостійна робота</td><td>110</td><td>122</td></tr>
<tr><td>Консультації год.</td><td>10</td><td>18</td></tr>
<tr><td>Форма контролю:</td><td colspan="2">залік</td></tr>
<tr><td colspan="2">Мова навчання</td><td colspan="3">українська</td></tr>
</table>

II. Інформація про викладача

Крестьянполь Любов Юріївна
Науковий ступінь: кандидат технічних наук
Вчене звання: доцент
Посада: доцент
Контактна інформація: : lkrestyanpol@gmail.com
Дні занять http://194.44.187.20/cgi-bin/timetable.cgi

III. Опис освітнього компонента

1. **Анотація**. Освітній компонент «Основи інформаційної безпеки» відноситься до циклу вибіркових ОК підготовки бакалаврів в галузі В Культура, мистецтво та гуманітарні науки, В11 Філологія, Прикладна лінгвістика. Переклад і комп'ютерна лінгвістика.

ВОК «Основи інформаційної безпеки» складається з лекцій, практичних занять та самостійної роботи здобувачів. Самостійна робота здобувачів в аудиторії здійснюється під час практичних занять, а також під час самостійного опрацювання лекційного матеріалу та підготовки до семінарів та заліку. Самостійна робота здобувачів поза університетом включає вивчення літературних джерел, матеріалу лекцій, підготовку до практичних занять, підготовку рефератів.

2. **Метою** викладання ВОК «Основи інформаційної безпеки» є ознайомлення здобувачів із базовими принципами та поняттями особистої інформаційної безпеки, та безпеки у сучасних інформаційних системах.

Завданнями вивчення ВОК є формування та розвиток навичок виявлення і протидії інформаційним загрозам на рівні людини, суспільства та держави. Здобувачі вищої освіти також вивчатимуть положення нормативно-правових актів, які спрямовані на забезпечення інформаційних прав та

свобод людини і громадянина та захист інтересів держави в інформаційній сфері.

Методи навчання. У ВОК застосовуються традиційні методи: пояснювально-ілюстративний, відповіді на запитання. Інноваційні: проєктно-дослідницький, використання інформаційних технологій. Здобувачі діляться на групи, яким дається комплекс завдань чи проблемне питання, визначений час і, можливо, додаткове оснащення для виконання. Метод спрямований на розвиток пошукових, аналітичних якостей здобувачів, а також навичок командної роботи.

3. Структура освітнього компоненту

Назви Змістових модулів і тем	**Денна форма**				**Заочна форма**			
	Лек.	**ПР.**	**Сам. роб.**	***Методи контролю/ Бали**	**Лек.**	**ПР.**	**Сам. роб.**	***Методи / Бали**
Змістовий модуль 1. Основні поняття інформаційної безпеки. Законодавчий та адміністративний рівні інформаційної безпеки								
Тема 1.Поняття та основні завдання інформаційної безпеки.	2	2	8	1	-	-	10	-
Тема 2. Види інформації, що підлягають захисту	-	2	8	1	2	2	10	8
Тема 3.Нормативно-правова база у сфері інформаційної безпеки.	2	2	8	2	-	-	10	8
Тема 4. Міжнародні стандарти у галузі інформаційної безпеки	-	2	8	4	-	-	10	-
Тема 5. Загрози інформаційній безпекці.	2	2	8	4	-	-	10	8
Змістовий модуль 2. Практичні аспекти інформаційної безпеки								
Тема 6. Основи управління інформаційною безпекою.	2	-	8	4	2	-	10	-
Тема 7. Соціальна інженерія.	-	2	8	4	-	-	10	-
Тема 8 Інсайдерство.	-	2	8	4	-	-	10	-
Тема 9. Інформаційне протиборство та інформаційна війна.	-	2	10	4	-	2	10	8
Тема 10. Інформаційна безпека у організаціях	2	-	12	4	-	-	10	-
Тема 11. Правове регулювання інформаційних відносин в сфері інтелектуальної власності.	-	2	12	4	-	2	10	8
Тема 12. Правове регулювання обігу інформації в Інтернет-мережі.	-	2	12	4	-	-	8	-
Тест				60				60
Всього годин/Балів	10	20	110	100	4	6	118	100

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

IV. Політика оцінювання

Оцінювання знань здобувачів освіти з ВОК здійснюється на основі результатів поточного і підсумкового контролю знань. Об'єктом оцінювання знань здобувачів освіти є програмовий матеріал, засвоєння якого перевіряється під час цих видів контролю. Оцінювання здійснюється за 100-бальною шкалою.

Детальніше про засади поточного та підсумкового оцінювання див. Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Волинського національного університету імені Лесі Українки.

Політика щодо відвідування. Сам факт відвідування лекцій та практичних робіт фіксується, але не оцінюється. Оцінюється виключно робота, яку здобувачі виконують на заняттях. За об'єктивних причин (наприклад, хвороба, міжнародне стажування, участь у конференціях, олімпіадах) навчання може відбуватись в онлайн формі (змішана форма навчання) за погодженням із керівником курсу.

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, не можуть бути оцінені на максимальний бал. Здобувачі мають змогу відпрацювати ті практичні роботи, на яких вони не відповідали. Відпрацювання здійснюється шляхом складання тестових завдань за темою заняття або відповіді на контрольні запитання до відповідної теми.

Учасники освітнього процесу, які здобувають освіту з використанням елементів дуальної форми навчання, повинні чітко дотримуватися індивідуального плану відповідно до Положення про підготовку здобувачів освіти у ВНУ імені Лесі Українки з використанням елементів дуальної форми здобуття освіти.

Позааудиторні заняття В межах вивчення ОК можлива участь у конференціях, форумах, круглих столах, олімпіадах відповідного спрямування. За участь у даних заходах здобувачам додаються додаткові бали до поточного оцінювання. За участь у проблемній групі, публікацію тез, участь у ІІ етапі Всеукраїнської студентської олімпіади або конкурсу наукових робіт – 5 балів. За участь у І етапі Всеукраїнської студентської олімпіади або конкурсу наукових робіт, призове місце у ІІ етапі Всеукраїнської студентської олімпіади або конкурсу наукових робіт, публікацію статті – 10 балів. За призове місце у І етапі Всеукраїнської студентської олімпіади або конкурсу наукових робіт – 15 балів.

Здобувачам можуть зараховуватись результати навчання отримані у формальній, неформальній освіті (професійні курси, тренінги, громадянська освіта, онлайн-освіта, стажування), за умови відповідності тематики курсу або заняття. Процес зарахування врегульований Положенням про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті ВНУ імені Лесі Українки і рішенням науково-

методичної комісії факультету іноземної філології (протокол № 7 від 03.02.2022 р.).

Політика щодо академічної доброчесності. Відповідно до статті 42 Закону України «Про освіту» під час навчання, викладання та провадження наукової діяльності учасники освітнього процесу повинні керуватися етичними принципами та правилами, визначеними законом, з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Жодні форми порушення академічної доброчесності (недбайливе цитування, присвоєння чужих ідей чи робіт, плагіат, псевдоавторство, неповажне ставлення до учасників освітнього процесу, списування тощо) недопустимі. Загальні засади, принципи, настанови та правила етичної поведінки учасників освітнього процесу у ВНУ імені Лесу Українки регульовано Кодексом академічної доброчесності ВНУ імені Лесі Українки.

Процедура оскарження результатів контрольних заходів. Здобувачі освіти мають право порушити будь-яке питання, яке стосується процедури проведення чи оцінювання контрольних заходів та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами у ЗВО (див. Положення про порядок і процедури вирішення конфліктних ситуацій ВНУ імені Лесі Українки, пункт 5 «ВРЕГУЛЮВАННЯ КОНФЛІКТІВ У НАВЧАЛЬНОМУ ПРОЦЕСІ»).

V. Підсумковий контроль

Відповідно до Положення про поточне та підсумкове оцінювання знань здобувачів оцінювання ВОК «Основи інформаційної безпеки» здійснюється за 100-бальною шкалою.

При вивченні ВОК «Основи інформаційної безпеки» передбачаються такі види контролю: поточний та підсумковий.

Поточний контроль здійснюється у вигляді усної відповіді на запитання під час захисту виконаних практичних робіт. Поточний контроль також застосовується для оцінювання виконання самостійної роботи у вигляді усної або письмової відповіді на контрольні запитання з теми даної на самостійне опрацювання. За поточну роботу разом із тестуванням протягом семестру здобувач може набрати максимум 100 балів. 40 балів за практичні роботи та 60 за тест. Тестування здійснюється після завершення усіх змістових модулів шляхом проходження тестових завдань.

Якщо здобувач протягом семестру набирає необхідні бали для зарахування ВОК, він може не здавати підсумковий контроль. Оцінка з ВОК виставляється як арифметична сума балів набраних за поточну роботу протягом семестру та балів набраних за тестування. Протягом семестру здобувач може набрати максимум 100 балів з ВОК. Мінімальний бал для зарахування заліку становить 60 балів. Якщо здобувач набирає менше як 60

балів, він складає залік під час ліквідації академічної заборгованості викладачу. У цьому випадку бали, набрані під час поточного оцінювання анульовуються. Максимальна кількість балів на залік під час ліквідації академічної заборгованості, як правило, 100. Залік включає 4 питання, кожне з яких оцінюється у 25 балів.

Процедура оскарження результатів контрольних заходів регламентується Положення про порядок і процедури вирішення конфліктних ситуацій ВНУ імені Лесі Українки, пункт 5 «ВРЕГУЛЮВАННЯ КОНФЛІКТІВ У НАВЧАЛЬНОМУ ПРОЦЕСІ»).

VI. Шкала оцінювання

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

Питання, завдання заліку

1. Дайте визначення інформаційної безпеки.
2. Які основні завдання інформаційної безпеки?
3. Поняття інформаційних ресурсів.
4. Принципи забезпечення інформаційної безпеки.
5. Класифікація інформації за рівнем доступу.
6. Персональні дані та їх захист.
7. Комерційна та державна таємниця: відмінності.
8. Конфіденційна інформація та відкриті дані.
9. Приклади інформації, що підлягає обов'язковому захисту.
10. Основні закони України у сфері інформаційної безпеки.
11. Закон України «Про інформацію»: ключові положення.
12. Закон України «Про захист персональних даних».
13. Роль Кіберполіції України у сфері кібербезпеки.
14. Відповідальність за порушення вимог інформаційної безпеки.
15. Стандарти ISO/IEC 27001, 27002: призначення та структура.
16. Концепція ризик-менеджменту за ISO 27005.
17. Європейське законодавство (GDPR): основні вимоги.
18. CIS Controls: характеристика та призначення.
19. Роль міжнародних стандартів у побудові системи інформаційної безпеки.

20. Класифікація загроз: внутрішні та зовнішні.
21. Шкідливе ПЗ: види та принципи дії.
22. DDoS-атаки: сутність і наслідки.
23. Порушення цілісності та доступності інформації: приклади.
24. Методи запобігання основним загрозам.
25. Поняття СОІБ (Система управління інформаційною безпекою).
26. Політика інформаційної безпеки: складові.
27. Аналіз ризиків як основа управління ІБ.
28. Ролі та відповідальність у системі ІБ.
29. Аудит інформаційної безпеки.
30. Поняття та види соціальної інженерії.
31. Фішинг, вішинг, смішинг: характеристика.
32. Психологічні прийоми впливу на людину.
33. Методи захисту від соціальної інженерії.
34. Приклади реальних атак соціальних інженерів.
35. Хто такий інсайдер у контексті ІБ?
36. Внутрішні загрози: причини виникнення.
37. Методи виявлення інсайдерської діяльності.
38. Політика мінімальних привілеїв.
39. Захист від інсайдерських загроз у організаціях.
40. Поняття інформаційної війни.
41. Засоби інформаційного впливу.
42. Кібероперації як елемент інформаційної війни.
43. Пропаганда та дезінформація: механізми.
44. Приклади сучасних інформаційних протиборств.
45. Розробка політик ІБ у організації.
46. Fsecurity Awareness Training: зміст та значення.
47. Контроль доступу та автентифікація.
48. Фізична безпека в організаціях.
49. Реагування на інциденти інформаційної безпеки.
50. Поняття інтелектуальної власності.
51. Авторське право та суміжні права.
52. Патентне право: основи.
53. Порушення прав інтелектуальної власності в цифровому середовищі.
54. Захист інтелектуальної власності на програмне забезпечення.
55. Правовий статус Інтернет-контенту.
56. Регулювання діяльності онлайн-платформ.
57. Кіберзлочини та їх правова кваліфікація.
58. Регулювання електронної комерції.
59. Відповідальність за порушення правил обробки даних в Інтернеті.

VI. Рекомендована література

Основна

1. Арістова І.В., Баранов О.А., Дзьобань О.В. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології. Київ: КВІЦ, 2019. 344 с.
2. Куліш А.М., Кобзєва Т.А., Шапіро В.С. Інформаційне право України : навч. посіб. Суми: Сумський державний університет, 2016. 108 с.
3. Сорока Н.Є. Авторське право і суміжні права в інформаційному суспільстві: європейський досвід : монографія. Харків : Право, 2019. 334с.
4. Marett P. Information Law in Practice. London: Routledge, 2017. https://doi.org/10.4324/9781315185187.
5. James Boyle, Jennifer Jenkins. Intellectual Property: Law & the Information Society – Cases and Materials. Duke Law School, 2016. https://web.law.duke.edu/cspd/pdf/IPCasebook2016.pdf.
6. Інформаційні технології в проектуванні системи захисту пакованої продукції : монографія / Б.О. Пальчевський, О.А. Крестьянполь, Л.Ю. Крестьянполь; за ред. проф. Б.О. Пальчевського. Луцьк : Вежа-Друк, 2015. 160 с.
7. Крестьянполь Л.Ю. Аналіз способів захисту інформації при несанкціонованому доступі з інтернету в локальну мережу. *Матеріали доповідей міжнародної науково-практичної конференції «Матеріали і покриття в екстремальних умовах: теоретичні і експериментальні основи технологій виготовлення».* Луцьк-Світязь 2017. С.102-104.
8. Krestyanpol L. Social engineering in the concept of rational and irrational consumer behavior. Front. Nutr. 2022. Vol. 9:961929. doi: 10.3389/fnut.2022.961929 (Scopus).
9. Дудикевич, В.Б., Хорошко В.О., Яремчук Ю.Є. Д81 Основи інформаційної безпеки : навч. пос. Вінниця : ВНТУ, 2018. 316 с. https://pdf.lib.vntu.edu.ua/books/IRVC/Dudikevich_2018_316.pdf
10. Інформаційна безпека. Підручник / В.В. Остроухов, М.М. Присяжнюк, О.І. Фармагей, М.М. Чеховська та ін.; під ред. В.В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с. https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf?srsltid=AfmBOoq97zqQA3MxV-I5Bcky_iea2hCT3BCXlHrIGt8yupvR-bg3HbEZ
11. Бурячок В.Л., Киричок Р.В., Складанний П.М. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. К., 2018. 320 с. https://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf
12. Навчальний курс на платформі Prometheus https://prometheus.org.ua/prometheus-free/info-security-basics

Стандарти

13. ISO/IEC 27001 – «Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційної безпеки – Вимоги». Міжнародний стандарт, базувався на BS 7799-2: 2005.
14. ISO/IEC 27002 – Зараз: ISO/IEC 17799: 2005. «Інформаційні технології – Технології безпеки – Практичні правила управління інформаційної безпеки». 2007.