

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

СИЛАБУС

Нормативного освітнього компонента

ЗАХИСТ ІНФОРМАЦІЇ

підготовки спеціальності освітньо-професійної програми	Бакалавра 035 Філологія Прикладна лінгвістика. Переклад і комп'ютерна лінгвістика
форма навчання	денна, заочна
курс	4
семестр	VII

Луцьк 2022

Силабус освітнього компонента «ЗАХИСТ ІНФОРМАЦІЇ» підготовки бакалавра, галузі знань 03 Гуманітарні науки, спеціальності 035 Філологія, за освітньою програмою **Прикладна лінгвістика. Переклад і комп'ютерна лінгвістика.**


Розробники: Крестьянполь Любов Юріївна, к.т.н., доцент, доцент кафедри прикладної лінгвістики.

Погоджено

Гарант освітньо-професійної програми:  (Бондар Т. Г.)

Силабус освітнього компонента затверджено на засіданні кафедри прикладної лінгвістики
протокол № 1 від 31. 08. 2021 р.

Силабус освітнього компонента перезатверджено на засіданні кафедри прикладної лінгвістики
протокол № 1 від 30. 08. 2022 р.

Завідувач кафедри:  (Біскуб І.П.)

I. Опис освітнього компонента

Таблиця 1.1 (денна форма)

Найменування показників	Галузь знань, спеціальність, освітня програма, освітній рівень	Характеристика освітнього компонента
Денна форма навчання	03 Гуманітарні науки 035 Філологія Прикладна лінгвістика Переклад і комп'ютерна лінгвістика Бакалавр	Нормативний
Кількість годин/кредитів 3/90		Рік навчання 4
		Семестр 7
		Лекції 10 год.
		Практичні (семінарські) 22 год.
		Самостійна робота 52 год.
		Консультації 6 год.
		Форма контролю: екзамен
Мова навчання		українська

Таблиця 1.2 (заочна форма)

Найменування показників	Галузь знань, спеціальність, освітня програма, освітній рівень	Характеристика освітнього компонента
Заочна форма навчання	03 Гуманітарні науки 035 Філологія Прикладна лінгвістика Переклад і комп'ютерна лінгвістика Бакалавр	Нормативний
Кількість годин/кредитів 3/90		Рік навчання 4
		Семестр 7
		Лекції 4 год.
		Практичні (семінарські) 10 год.
		Самостійна робота 64 год.
		Консультації 12 год.
		Форма контролю: екзамен
Мова навчання		українська

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://94.130.69.82/cgi-bin/timetable.cgi?n=700>

III. Опис освітнього компонента

1. **Анотація.** ОК «Захист інформації» відноситься до нормативних ОК підготовки бакалаврів в галузі 03 Гуманітарні науки, 035 Філологія, Прикладна лінгвістика. Переклад і комп'ютерна лінгвістика.

ОК «Захист інформації» складається з лекцій, практичних занять та самостійної роботи здобувачів. Самостійна робота здобувачів в аудиторії здійснюється під час лабораторних 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 лабораторних занять, підготовку рефератів.

2. **Пререквізити.** Вивчення ОК «Захист інформації» передбачає володіння знаннями, які отримані здобувачами при вивченні ОК «Інформаційні технології», ОК «Основи WEB UI розробки», ОК «Математичне моделювання», ОК «Програмування і бази даних».

3. **Метою** викладання ОК «Захист інформації» є навчання здобувачів принципам забезпечення інформаційної безпеки, як однієї з найважливіших сфер діяльності в умовах формування інформаційного суспільства, опанування основними термінами та категоріями інформаційної безпеки на рівні їх тлумачення та відтворення для практичного застосування та втілення у процесі професійної діяльності..

Завданнями вивчення ОК «Захист інформації» є:

- надати вичерпну та актуальну інформацію про комплекс сучасних інформаційно-комунікаційних технологій;
- сформувані у студентів високий рівень інформаційно-технологічної компетентності;
- сформувані у здобувачів уміння розуміти та розв'язувати поставлені перед ними задачі вибору технічних та програмних засобів захисту інформації;
- сформувані у здобувачів навички пошуку нових шляхів розв'язання поставлених перед ними задач із врахуванням зміни технологій та вимог суспільства;
- залучити майбутніх фахівців до опрацювання спеціальної науково-методичної літератури, що має стати джерелом постійної роботи над собою з метою підвищення рівня професійної кваліфікації.

Завдання вивчення ОК визначаються вимогами освітньо – професійної програми підготовки бакалаврів зі спеціальності 035 Філологія, прикладна лінгвістика. Переклад і комп'ютерна лінгвістика і включають придбання загальних (ЗК) та фахових (ФК) компетентностей.

Методи навчання. У ОК застосовуються традиційні методи: пояснювально-ілюстративний, відповіді на запитання. Інноваційні: використання інформаційних технологій. Практичні роботи із застосуванням інформаційних технологій (Google Workspace, WinZip, WinRar, Advanced PDF

Password Recovery, Wolfram Mathematica). 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.

4. **Результати навчання.**

Загальні компетентності (ЗК):

- **ЗК 3.** Здатність спілкуватися державною мовою як усно, так і письмово
- **ЗК 5.** Здатність учитися й оволодівати сучасними знаннями.
- **ЗК6.** Здатність до пошуку, опрацювання та аналізу інформації з різних джерел.
- **ЗК7.** Уміння виявляти, ставити та вирішувати проблеми.
- **ЗК8.** Здатність працювати в команді та автономно.
- **ЗК 10.** Здатність до абстрактного мислення, аналізу та синтезу.
- **ЗК 11.** Здатність застосовувати знання у практичних ситуаціях.
- **ЗК 12.** Навички використання інформаційних і комунікаційних технологій.

Фахові компетентності (ФК):

- **ФК8.** Здатність вільно оперувати спеціальною термінологією для розв'язання професійних завдань.
- **ФК 15.** Здатність використовувати сучасні інформаційні системи та технології під час виконання функціональних завдань та обов'язків, знати основи безпечної роботи в інформаційних системах, методи створення баз даних та вебресурсів
- **ФК 17.** Здатність використовувати базові знання розділів математики та логіки у завданнях комп'ютерної лінгвістики та розробці програмного забезпечення.

Даний ОК формує такі програмні результати навчання (ПРН):

- **ПРН 1.** Вільно спілкуватися з професійних питань із фахівцями та нефхівцями державною та іноземними мовами усно й письмово, використовувати їх для організації ефективної міжкультурної комунікації.
- **ПРН 2.** Ефективно працювати з інформацією: добирати необхідну інформацію з різних джерел, зокрема з фахової літератури та електронних баз, критично аналізувати й інтерпретувати її, впорядковувати, класифікувати й систематизувати.
- **ПРН 3.** Організовувати процес свого навчання й самоосвіти.
- **ПРН 6.** Використовувати інформаційні й комунікаційні технології для вирішення складних спеціалізованих задач і проблем професійної діяльності.
- **ПРН 18.** Мати навички управління комплексними діями або проектами при розв'язанні складних проблем у професійній діяльності в галузі обраної філологічної спеціалізації та нести відповідальність за прийняття рішень у непередбачуваних умовах.

- **ПРН 22.** Застосовувати знання із логіки, технологій моделювання, експертних систем і технологій штучного інтелекту при розв'язанні задач проектування та управління інформаційними системами.

5. Структура освітнього компонента

Назви Змістових модулів і тем	Денна форма				Заочна форма				*Методи контролю/ Бали
	Лек.	Пр.	Сам. роб.	Конс.	Лек.	Пр.	Сам. роб.	Конс.	
Змістовий модуль 1. Безпека інформаційних технологій									
Тема 1. Тема 1. Загальні аспекти захисту інформації. Огляд безпеки системи. Основні поняття та визначення безпеки. Види інформаційних систем з точки зору захисту інформації. Класифікація загроз для інформації та їх джерел. Класифікація основних засобів протидії загрозам безпеки.	2	-	2	-	2	-	4	-	ДС+РЗ /К 2 бали
Тема 2. Аудит безпеки інформаційної системи.	-	2	4	2	-	-	4	2	ДС+РЗ /К 4 бали
Тема 3. Основи технічного захисту інформації. Види захисту інформації. Комплексна система захисту інформації. Захист інформації від несанкціонованого доступу. Захист інформації від витоку технічними каналами.	2	-	2	-	-	-	4	2	ДС+РЗ /К 2 бали
Тема 4. Збереження цілісності інформації методами архівування.	-	2	2	2	-	2	4	-	ДС+РЗ /К 2 бали
Тема 5. Вивчення засобів захисту та зламу PDF-документів	-	2	2	-	-	-	4	2	ДС+РЗ /К 2 бали
Тема 6. Захист даних від несанкціонованого доступу та пошкоджень.	-	2	2	-	-	-	4	2	ДС+РЗ /К 2 бали
Тема 7. Створення стійких паролів для PDF-документів,	-	2	2	-	-	-	4	2	ДС+РЗ /К 2 бали

архівів, текстових документів.									
Тема 8. Використання облікових записів для реалізації політики безпеки.	-	2	4	-	-	-	4	2	ДС+РЗ /К 2 бали
Тема 9. Налаштування захисту flash носіїв.	-	2	4	-	-	2	4	-	ДС+РЗ /К 2 бали
Змістовий модуль 2. Інформаційна безпека автоматизованих систем і комунікаційних мереж									
Тема 10. Шифрування даних. Загальне поняття шифрування даних. Перші шифри. Ключі шифрування. Алгоритми шифрування. Шифрування з симетричними та асиметричним ключами.	2	-	4	-	2	-	4	-	ДС+РЗ /К 2 бали
Тема 11. Шифрування тексту методом стовпцевої перестановки та подвійної перестановки	-	2	4	2	-	2	4	-	ДС+РЗ /К 4 бали
Тема 12. Використання шифру Віженера для захисту даних у MSExcel.	-	2	4	-	-	-	4	-	ДС+РЗ /К 4 бали
Тема 13. Частотний аналіз тексту за допомогою програмного продукту Wolfram Mathematica.	-	2	4	-	-	2	4	-	ДС+РЗ /К 4 бали
Тема 14. Основи безпечної роботи в мережі «Інтернет».	2	-	4	-	-	-	4		ДС+РЗ /К 2 бали
Тема 15. Налаштування параметрів безпеки веббраузерів.	-	2	4	-	-	-	4		ДС+РЗ /К 2 бали
Тема 16. Комп'ютерна вірусологія. Поняття комп'ютерного вірусу та його історія виникнення. Ознаки комп'ютерних вірусів. Види комп'ютерних вірусів. Аналітика	2	-	4	-	2	2	4		ДС+РЗ /К 2 бали
Всього годин/Балів	10	22	52	6	4	10	64	12	40

* Методи контролю: ДС – дискусія, ДБ – дебати, Т – тести, РМГ – робота в малих групах, МКР / КР – модульна контрольна робота/ контрольна робота, аналітичне есе, аналіз твору.

6. Завдання для самостійного опрацювання

	Назва теми	Кількість годин (денна форма)	Кількість годин (заочна форма)
Тема 1	Поняття управління інформаційною безпекою. Основи інформаційної державної політики у сфері інформаційної безпеки.	2 год.	4 год.
Тема 2	Основні завдання міжнародних стандартів інформаційної безпеки. Вимоги стандартів ISO 27001 та ISO 27002 щодо розробки системи управління інформаційною безпекою.	4 год.	4 год.
Тема 3	Процес виявлення нових ризиків інформаційної безпеки. Сертифікація продуктів інформаційної безпеки. Розробка та впровадження системи управління інформаційною безпекою.	4 год.	4 год.
Тема 4	Інформаційні системи та технології як об'єкти інформаційної безпеки. Захист у базах даних та операційних системах. Заходи з моніторингу та перевірки системи управління інформаційною безпекою.	4 год.	4 год.
Тема 5	Процес управління ризиками: мета та завдання.	4 год.	4 год.
Тема 6	Призначення та принцип роботи апаратного та програмного забезпечення для захисту інформації.	4 год.	4 год.
Тема 7	Створення комплексної системи захисту інформації. Вимоги до комплексної системи захисту інформації та політики безпеки.	4 год.	4 год.
Тема 8	Поняття стійкості паролю.	4 год.	4 год.
Тема 9	Захист у базах даних та операційних системах. Запобігання проникненню та доступу на рівні користувачів, управління на рівні каналів зв'язку.	4 год.	4 год.
Тема 10	Робота з накопичувачами інформації. Захист від модифікації, знищення та несанкціонованого доступу.	4 год.	4 год.
Тема 11	Криптографічний алгоритм. Основні криптографічні методології з ключем.	4 год.	4 год.
Тема 12	Загальні вимоги до криптографічних систем захисту інформації.	2 год.	4 год.
Тема 13	Ключові моменти криптоаналізу. Способи злому шифру.	2 год.	4 год.
Тема 14	Алгоритм цифрового підпису.	2 год.	4 год.
Тема 15	Функції фільтруючого маршрутизатора, його недоліки та переваги.	2 год.	4 год.

Тема 16	Класифікація шкідливого програмного забезпечення.	2 год.	4 год.
Всього		52	64

IV. Політика оцінювання

Оцінювання знань здобувачів освіти з ОК «Захист інформації» 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. Перескладання модульних контрольних робіт чи підсумкових робіт відбувається згідно «Положення про поточне та підсумкове оцінювання знань студентів Волинського національного університету імені Лесі Українки».

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 II етапі Всеукраїнської студентської олімпіади або конкурсу наукових робіт – 5 балів. За участь у I етапі Всеукраїнської студентської олімпіади або конкурсу наукових робіт, призове місце у II етапі Всеукраїнської студентської олімпіади або конкурсу наукових робіт, публікацію статті – 10 балів. За призове місце у II 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 Волинського національного університету 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 у ВНУ імені Лесі Українки](#), пункт 5 «ВРЕГУЛЮВАННЯ КОНФЛІКТІВ У НАВЧАЛЬНОМУ ПРОЦЕСІ»).

V. Підсумковий контроль

Оцінювання ОК «Захист інформації» здійснюється за 100-бальною шкалою.

При вивченні ОК «Захист інформації» передбачаються такі види контролю: поточний та підсумковий.

Поточний контроль здійснюється у вигляді усної відповіді на контрольні 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 протягом семестру здобувач може набрати максимум 40 балів.

Підсумковий контроль проходить у вигляді екзамену після закінчення вивчення ОК. Максимальна кількість балів яку може отримати здобувач за підсумковий контроль складає 60 балів.

Протягом семестру здобувач може набрати максимум 100 балів з Якщо сума балів, яку отримав здобувач освіти, є меншою ніж 60 балів, то він складає

підсумковий семестровий контроль повторно в терміни, визначені розкладом заліково-екзаменаційної сесії.

Розподіл балів, які отримують здобувачі

Поточний контроль (має 40 балів)		Підсумковий контроль (має 60 балів)	Загальна кількість балів
Змістовий модуль 1 Т1-Т9	Змістовий модуль 2 Т10-Т16	Екзамен	100
20	20	60	

VI. Шкала оцінювання

Оцінка в балах за всі види навчальної діяльності	Оцінка
90 – 100	Відмінно
82 – 89	Дуже добре
75 - 81	Добре
67 -74	Задовільно
60 - 66	Достатньо
1 – 59	Незадовільно

VII. Рекомендована література

Основна література

1. Браїловський М.М. Захист інформації у банківській діяльності / М.М. Браїловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ “Поліграф Консалтинг”, 2004. – 216 с.
2. Гундарь К. Ю. та ін. Защита информации в компьютерных системах / К. Ю. Гундарь, А. Ю. Гундарь, Д. А. Янишевский. – К.: «Корнійчук», 2000. – 152 с.
3. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Людмила Ярославівна Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с
4. Information technology. Security techniques. Information security management systems – Requirements: ISO/IEC 27001:2017
5. Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів: ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT)
6. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. — [Чинний

від 28.04.1999]. — К.: ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації): <https://tzi.com.ua/downloads/1.1-003-99.pdf>

7. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. — Чинний з 29.12.2014 р. ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. — 228 с.

8. Nagle F., Ransbotham S., Westerman G. The Effects of Security Management on Security Events, WEIS, 2017.

9. NIST (National Institute Of Standards And Technology). 1995. An Introduction to Computer Security: The NIST Handbook. (Special Publication 800-12).

10. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. — Чинний з 28.04.1999. — К.: ДСТСЗІ СБ України, 1999. — 14 с.

11. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. — Чинний з 28.04.1999. — К.: ДСТСЗІ СБ України, 1999. — 53 с.

12. Кузнецов О. О. Захист інформації в інформаційних системах: навч. посіб. / О.О. Кузнецов, С.П. Євсєєв, О.Г. Король. — Харків: ХНЕУ, 2011. — 510 с.

13. Остапов С.Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсєєв, О.Г. Король. — Х.: ХНЕУ, 2013. — 476 с.

14. Про захист інформації в інформаційно-комунікаційних системах: Закон України від № 80/94ВР. Відомості Верховної Ради України. 1994. № 31. ст. 286. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр>

15. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. — Київ: КПІ ім. Ігоря Сікорського, 2018. — 162 с.

Додаткова література

1. Кавун С. В. Информационная безопасность в бизнесе: науч. Изд. Харьков: Изд. ХНЕУ, 2007. — 408 с.
2. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. — Х.: ХНЕУ, 2013. — 476 с. URL: <https://www.twirpx.com/file/2340575/>
3. Хорошко В. О. Основи інформаційної безпеки: підручник / В. О. Хорошко, В. С. Чередниченко, М. Є. Шелест; за ред. В. О. Хорошка. — К.: ДУІКТ, 2008. — 186 с.
4. Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України: нормативно-правова база. — Режим доступу: www.dststzi.gov.ua/dststzi/control/uk/index