МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ ІМЕНІ ЛЕСІ УКРАЇНКИ
Факультет іноземної філології
Кафедра прикладної лінгвістики

СИЛАБУС
вибіркової навчальної дисципліни

ЗАХИСТ ІНФОРМАЦІЇ

підготовки	бакалавра
спеціальності	035 Філологія
освітньо-професійна програма	Прикладна лінгвістика. Переклад і комп'ютерна лінгвістика
форма навчання	Денна, заочна
курс	4-й
семестр	VIII

Луцьк 2020

Силабус навчальної дисципліни «Захист інформації» підготовки бакалавра, галузі знань 03 Гуманітарні науки, спеціальності 035 Філологія, за освітньою-професійною програмою Прикладна лінгвістика. Переклад і комп'ютерна лінгвістика.

Розробник: Крестьянполь Любов Юріївна доцент, к.т.н., доцент.

Силабус навчальної дисципліни затверджено на засіданні кафедри прикладної лінгвістики

протокол № 2 від 23. 09. 2020 р.

Завідувач кафедри:_____Біскуб І.П.

©Крестьянполь, Л.Ю., 2020р.

І. Опис навчальної дисципліни

Таблиця 1.1 (денна форма)

Найменування показників	Галузь знань, спеціальність, освітня програма, освітній рівень	Характеристика навчальної дисципліни
Денна форма навчання	**03 Гуманітарні науки 035 Філологія Прикладна лінгвістика Переклад і комп'ютерна лінгвістика Бакалавр**	**Вибіркова**
		Рік навчання 4
Кількість годин/кредитів 3/90		**Семестр** 8-ий
		Лекції 16 год.
		Практичні (семінарські) 12 год.
		Самостійна робота 56 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 навчальної дисципліни
Заочна форма навчання	**03 Гуманітарні науки 035 Філологія Прикладна лінгвістика Переклад і комп'ютерна лінгвістика Бакалавр**	**Вибіркова**
		Рікнавчання 4
Кількість годин/кредитів 3/90		**Семестр** 8-ий
		Лекції 6 год.
		Практичні (семінарські) 4 год.
		Самостійна робота 68 год.
		Консультації 12 год.
		Форма контролю: залік
Мова навчання		**українська**

ІІ. 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

ІІІ. Опис дисципліни

1. **Анотація**. Навчальна дисципліна “Захист інформації” відноситься до циклу вибіркових дисциплін підготовки бакалаврів в галузі 03

Гуманітарні науки, 035 Філологія, Прикладна лінгвістика. Переклад і комп'ютерна лінгвістика.

Дисципліна «Захист інформації» складається з лекцій, практичних занять та самостійної роботи студентів. Самостійна робота студентів в аудиторії здійснюється під час лабораторних занять, а також під час самостійного опрацювання лекційного матеріалу та підготовки до семінарів та заліку. Самостійна робота студентів поза університетом включає вивчення літературних джерел, матеріалу лекцій, підготовку до лабораторних занять, підготовку рефератів.

2. **Пререквізити**. Вивчення дисципліни «Захист інформації» передбачає володіння знаннями, які отримані студентами при вивченні курсів:
   - Інформаційні технології;
   - Основи WEB UI розробки;
   - Математичне моделювання;
   - Програмування і бази даних.
3. **Метою** викладання навчальної дисципліни «Захист інформації» є навчання студентів 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 дисципліни «Захист інформації» є:
   - надати вичерпну та актуальну інформацію про комплекс сучасних інформаційно-комунікаційних технологій;
   - сформувати у студентів високий рівень інформаційно-технологічної компетентності;
   - сформувати у студентів уміння розуміти та розв’язувати поставлені перед ним задачі вибору технічних та програмних засобів захисту інформації;
   - сформувати у студентів навики 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 дисципліни визначаються вимогами освітньо – професійної програми підготовки бакалаврів зі спеціальності 035 Філологія, прикладналінгвістика. Переклад і комп'ютерна лінгвістика і включають придбання загальних (ЗК) та фахових (ФК) компетентностей.

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 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 13. Здатність застосовувати інформаційні технології у ході створення, впровадження та експлуатації інформаційних систем.
- ФК 14. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних), методики й техніки під час виконання функціональних завдань та обов'язків.
- ФК 15. Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет).

До кінця навчання студенти будуть компетентними з таких питань:

- володіння основними положеннями законодавства в галузі захисту інформації, міжнародних та національних стандартів безпеки інформаційних технологій (ІТ);
- реалізаціямеханізмів та протоколів забезпечення конфіденційності, автентичності та цілісності даних ІТ;
- використання програмних та апаратних засобів розмежування доступу до інформації у автоматизованих системах та антивірусних засобів захисту інформації у персональних комп'ютерах;
- проведення аналізу безпеки комп'ютерної системи та усунення можливих шляхів несанкціонованого доступудо інформації;
- реалізація організаційних та програмних заходів щодо підвищення рівня безпеки зберігання інформації;
- володіння основними положеннями адміністрування прав доступу до комп'ютерної системи з метою перешкоджання призначення невиправданих привілеїв;
- володіння основними положеннями застосування криптографічних методів та засобів захисту інформації;
- здійснення моніторингу системи з метою пошуку програмних закладок та каналів витоку інформації.

Даний курс формує наступніпрограмні результати навчання (ПРН):

- ПРН 1. Вільно спілкуватися з професійних питань із фахівцями та нефахівцями 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 проєктами при розв’язанні складних проблем у професійній діяльності в галузі обраної філологічної спеціалізації та нести відповідальність за прийняття рішень у непередбачуваних умовах.
- ПРН 20. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів для розв’язання задач проєктування і побудови інформаційних систем.

5. Структура навчальної дисципліни.

Назви Змістових модулів і тем	**Денна форма**				**Заочна форма**				
	Лек.	**Пр.**	**Сам. роб.**	**Конс.**	**Лек.**	**Пр.**	**Сам. роб.**	**Конс.**	***Форма контролю/ Бали**
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. Класифікаціязагроз для інформації та їхджерел. Класифікаціяосновнихзасобівпротидіїз агрозамбезпеки.	2	-	2	-	2	-	4	-	2
Тема 2. Аудит безпеки інформаційної системи.	-	2	4	2	-	-	4	2	4
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	2
Тема 4. Збереження цілісності	-	2	2	2	-	-	4	-	2

інформації методами архівування.									
Тема 5.Вивчення засобів захисту та зламу PDF-документів	-	2	2	-	-	-	4	2	2
Тема 6.Захистданих від несанкціонованого доступу та пошкоджень.	-	2	4	-	-	-	4	2	2
Тема 7.Створення стійких паролів для PDF-документів, архівів, текстових документів.	-	2	4	-	-	-	4	2	2
Тема 8. Використання облікових записів для реалізації політики безпеки.	-	-	4	-	-	-	4	2	2
Тема 9. Налаштування захисту flash носіїв.	-	-	4	-	-	-	4	-	2
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	-	2
Тема 11. Шифрування тексту методом стовпцевої перестановки та подвійної перестановки	-	2	4	2	-	-	4	-	4
Тема 12. Використання шифру Віженера для захисту даних у MSExcel.	-	2	4	-	-	-	4	-	4
Тема 13. Частотний аналіз тексту за допомогою програмного продукту Wolfram Mathematica.	2	-	4	-	-	2	6	-	4
Тема 14. Основи безпечної роботи в мережі «Інтернет».	2	-	4	-	-	-	6	-	2
Тема 15. Налаштування параметрів безпеки веббраузерів.	2	-	4	-	-	-	6	-	2
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	6	-	2
Разом	14	12	56	6	4	4	68	12	40
Види підсумкових робіт*(за потреби, на розсуд викладача, кафедри)*									
Модульна контрольна робота									
ІНДЗ									
Інше (вказати)									
Всього годин/Балів	14	12	56	6	4	4	68	12	40

*Форма 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.

6. Завдання для самостійного опрацювання.

Тема 1	Поняття управління інформаційною безпекою. Основи інформаційної державної політики у сфері інформаційної безпеки.	2 год..
Тема 2	Основні завдання міжнародних стандартів інформаційної безпеки. Вимоги стандартів ISO 27001 та ISO 27002 щодо розробки системи управління інформаційною безпекою.	4 год.
Тема 3	Процес виявлення нових ризиків інформаційної безпеки. Сертифікація продуктів інформаційної безпеки. Розробка та впровадження системи управління інформаційною безпекою.	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.
Тема 5	Процес управління ризиками: мета та завдання.	4 год.
Тема 6	Призначення та принцип роботи апаратного та програмного забезпечення для захисту інформації.	4 год.
Тема 7	Створення комплексної системи захисту інформації. Вимоги до комплексної системи захисту інформації та політики безпеки.	4 год.
Тема 8	Поняття стійкості паролю.	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.
Тема 10	Робота з накопичувачами інформації. Захист від модифікації, знищення та несанкціонованого доступу.	4год.
Тема 11	Криптографічний алгоритм. Основні криптографічні методології з ключем.	4 год.
Тема 12	Загальні вимоги до криптографічних систем захисту інформації.	2 год.
Тема 13	Ключові моменти криптоаналізу. Способи злому шифру.	2 год.
Тема 14	Алгоритм цифрового підпису.	2 год.
Тема 15	Функції фільтруючого маршрутизатора, його недоліки та переваги.	2 год.
Тема 16	Класифікація шкідливого програмного забезпечення.	2 год.

IV. Політика оцінювання

Політика щодо відвідування. Сам факт відвідування лекцій та практичних робіт фіксується, але не оцінюється. Оцінюється виключно робота, яку студенти 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».

Студенти 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. Відпрацювання «оптом» в кінці семестру не приймаються і не зараховуються.

За умови участі студентів у навчанні з елементами дуальної освіти передбачено можливість самостійного опрацювання студентами матеріалів навчальних занять протягом одного дня на тиждень та зарахування їх результатів до загальної кількості балів поточного контролю.

Процедура оскарження результатів контрольних заходів. Студенти мають можливість 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.

Позааудиторні заняття В межах вивчення навчальної дисципліни можлива участь у конференціях, форумах, круглих столах, олімпіадах відповідного спрямування. За участь у даних заходах студентам додаються додаткові бали (5 балів) до поточного оцінювання.

Студентам 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 визначення результатів навчання, отриманих у формальній, неформальній та / або інформальній освіті ВНУ імені Лесі Українки.

Політикащодоакадемічноїдоброчесності. Списування під час контрольних, модульних робітта екзаменів заборонені (в т. ч. із використанням мобільних пристроїв).

Дотримання академічної доброчесності, згідно Кодексу академічної доброчесності Волинського національного університету імені Лесі Українки, здобувачами освіти передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового

- контролю результатів навчання (для осіб з особливими освітніми потребами ця вимогазастосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень,відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової,творчої) діяльності, використані методики досліджень і джерела інформації.

Основні види відповідальності здобувачів освіти за порушенняакадемічної доброчесності (ч.6 статті 42 Закону України «Про освіту») :

- повторне проходження оцінювання (контрольна робота, іспит, залік
- тощо);
- повторне проходження відповідного освітнього компонента освітньої
- програми;
- відрахування з університету (крім осіб, які здобувають загальну середню
- освіту);
- позбавлення академічної стипендії;
- позбавлення наданих університетом пільг з оплати навчання.

V. Підсумковий контроль

При вивченні курсу “Захист інормації” передбачаються такі види контролю: поточний, модульний та підсумковий.

Поточний контроль здійснюється у вигляді усної відповіді на контрольні запитання під час захисту виконаних практичних робіт. Також поточний контроль застосовується стосовно виконання самостійної роботи у вигляді усної або письмової відповіді на контрольні запитання з теми даної на самостійне опрацювання. За поточну роботу протягом семестру студент може набрати максимум 40 балів (по 20 балів у кожному модулі).

Модульний контроль здійснюється стосовно теоретичного (лекційного) курсу у вигляді модульних контрольних робіт після завершення кожного з 2-х модулів шляхом письмової відповіді на контрольні питання або тестові завдання по модулю. За модульні контрольні роботи протягом семестру студент може набрати максимум 60 балів (по 30 балів у кожному модулі).

Оцінка з предмета виставляється як арифметична сума балів набраних за поточну роботу протягом двох модулів та балів набраних за дві модульні контрольні роботи. Протягом семестру студент може набрати максимум 100

балів. Якщо студента задовольняє отримана сума балів то процедура підсумкового контролю полягає лише у сумуванні цих балів. Якщо студент не згідний зі своєю оцінкою він може здавати підсумковий екзамен. Якщо студент не виконував протягом семестру практичні роботи та не має поточного балу, підсумковий контроль він може скласти лише на 60 балів.

Розподіл балів, які отримують студенти

<table>
<tr><td></td><td colspan="4">Поточне тестування та самостійна робота</td><td rowspan="2">Сума</td></tr>
<tr><td colspan="2">Модуль №1</td><td colspan="2">Модуль №2</td><td rowspan="2">Складання екзамену</td></tr>
<tr><td colspan="2">Т1-9</td><td colspan="2">Т10-16</td><td rowspan="3">100</td></tr>
<tr><td>Поточний контроль</td><td>МКР</td><td>Поточний контроль</td><td>МКР</td><td rowspan="2">60</td></tr>
<tr><td>20</td><td>30</td><td>20</td><td>30</td></tr>
</table>

VI.Шкала оцінювання

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

Рекомендована література та інтернет-ресурси

1. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ “Поліграф Консалтинг”, 2004. – 216 с.
2. Information technology. Security techniques. Information security management systems – Requirements: ISO/IEC 27001:2017
3. Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів: ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT)
4. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. — [Чинний від28.04.1999]. — К.: ДСТСЗІ СБУ, 1999. — No 22. — (Нормативний документ системи технічного захисту інформації): https://tzi.com.ua/downloads/1.1-003-99.pdf
5. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симметричного блокового перетворення. – Чинний з 29.12.2014 р. ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. – 228 с.
6. Nagle F., Ransbotham S., Westerman G. The Effects of Security Management on Security Events, WEIS, 2017.
7. NIST (National Institute Of Standards And Technology). 1995. An Introduction to Computer Security: The NIST Handbook. (Special Publication

800-12).

8. 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.

9. 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.

10. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Людмила Ярославівна Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с

11. Кузнецов О. О. Захист інформації в інформаційних системах: навч. посіб. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Харків: ХНЕУ, 2011. – 510 с.

12. Остапов С.Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с.

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

14. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. – Київ: КПІ ім. ІгоряСікорського, 2018. – 162 с.