

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

**СИЛАБУС**  
**нормативного освітнього компонента**

**ЗАХИСТ ІНФОРМАЦІЇ**

**підготовки здобувачів освіти першого (бакалаврського) рівня**

**галузі знань В Культура, мистецтво та гуманітарні науки**

**спеціальності В 11 Філологія**

**спеціалізації В 11.10 Прикладна лінгвістика**

**освітньо-професійної програми**

**Прикладна лінгвістика. Переклад**

**і комп'ютерна лінгвістика**

**Силабус освітнього компонента ЗАХИСТ ІНФОРМАЦІЇ** підготовки здобувачів освіти першого (бакалаврського) рівня, галузі знань В Культура, мистецтво та гуманітарні науки, спеціальності В11 Філологія, спеціалізації В 11.10 Прикладна лінгвістика, ОПП Прикладна лінгвістика. Переклад і комп'ютерна лінгвістика.

**Розробники:** Крестьянполь Любов Юріївна, к.т.н., доцент, доцент кафедри прикладної лінгвістики;  
Бендовський Григорій Валерійович, керівник лабораторії цифрової криміналістики Gross.

**Погоджено**

Гарант освітньо-професійної програми:  (Калиновська І. М.)

**Силабус освітнього компонента перезатверджено** на засіданні кафедри прикладної лінгвістики протокол № 1 від 31. 08. 2025 р.

В.о. завідувачки кафедри:  доц. І.М. Калиновська

## I. Опис освітнього компонента

Таблиця 1.1 (Денна форма)

Найменування показників	Галузь знань, спеціальність, освітня програма, освітній рівень	Характеристика освітнього компонента
Денна форма здобуття освіти	В Культура, мистецтво та гуманітарні науки  В11 Філологія  Прикладна лінгвістика. Переклад і комп'ютерна лінгвістика.  Бакалавр	Нормативний
Кількість годин/кредитів 90 / 3		Рік навчання: 4-й
		Семестр: 8-й
		Лекції: 12 год.
		Практичні (семінарські): 20 год.
		Самостійна робота: 52 год.
		Консультації: 6 год.
Мова навчання	українська	
	Форма контролю: залік	

## II. Інформація про викладачів

- Крестьянполь Любов Юріївна  
Науковий ступінь: кандидат технічних наук  
Вчене звання: доцент  
Посада: доцент  
Контактна інформація: lkrestyanpol@gmail.com
- Бендовський Григорій Валерійович, керівник лабораторії цифрової криміналістики Gross
- Дні занять <http://194.44.187.20/cgi-bin/timetable.cgi>

## III. Опис освітнього компонента

1. **Анотація.** ОК Захист інформації відноситься до нормативних ОК підготовки бакалаврів в галузі В Культура, мистецтво, гуманітарні науки В11 Філологія, спеціалізації В 11.10 Прикладна лінгвістика, ОПП 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 та навичками, набутими здобувачами освіти при вивченні ОК Інформаційно-комунікаційні технології, ОК Математичне моделювання, ОК Математична логіка, ОК Програмування, ОК Штучний інтелект та прикладні інформаційні технології.

3. **Метою** 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 в контексті захисту інформації; сформувати у здобувачів високий рівень інформаційно-технологічної компетентності; сформувати у здобувачів уміння розуміти та розв'язувати поставлені перед ними задачі вибору технічних та програмних засобів захисту інформації; сформувати у здобувачів навички пошуку нових шляхів розв'язання поставлених перед ними задач із врахуванням зміни технологій та вимог суспільства в контексті захисту інформації; 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 набуття загальних та фахових компетентностей.

**Методи навчання.** При вивченні ОК застосовуються традиційні методи: пояснювально-ілюстративний, запитання-відповіді. Інноваційні: використання інформаційних технологій, проблемно-пошуковий (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).

**Soft Skills** даного ОК корелюють із загальними та фаховими компетентностями визначеними Стандартом вищої освіти України: перший (бакалаврський) рівень, галузь знань 03 Гуманітарні науки, спеціальність 035 «Філологія».

#### 4. Результати навчання:

*Інтегральна компетентність:*

здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в галузі філології (лінгвістики, літературознавства, фольклористики, перекладу) в процесі професійної діяльності або навчання, що передбачає застосування теорій та методів філологічної науки і характеризується комплексністю та невизначеністю умов.

*Загальні компетентності (ЗК):*

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

**ЗК 5.** Здатність учитися й оволодівати сучасними знаннями.

**ЗК 6.** Здатність до пошуку, опрацювання та аналізу інформації з різних джерел.

**ЗК 7.** Уміння виявляти, ставити та вирішувати проблеми.

**ЗК 8.** 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.

**ЗК 14.** Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

*Фахові компетентності (ФК):*

**ФК 8.** 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 математичної логіки та моделювання 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 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.** Організувати 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 21.** 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 прикладних завдань у професійній діяльності.

**ПРН 22.** Застосовувати знання з математичної логіки, технологій моделювання, експертних систем і технологій штучного інтелекту при розв'язанні задач проєктування і використання інформаційних систем та технологій.

## 5. Структура освітнього компонента

Назви змістових модулів і тем	Усього	Лек.	Пр.	Сам. роб.	Конс.	*Форма контролю/ Бали
<b>Змістовий модуль 1. Безпека інформаційних технологій</b>						
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.	<b>6</b>	2	-	4	-	ДС+РЗ /К 2 бали
Тема 2. Аудит безпеки інформаційної системи.	<b>8</b>	-	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 витіку технічними каналами.	<b>6</b>	2	-	4	-	ДС+РЗ /К 2 бали
Тема 4. Збереження цілісності інформації методами архівування.	<b>8</b>	-	2	4	2	ДС+РЗ /К 2 бали
Тема 5. Вивчення засобів захисту та зламу PDF-документів	<b>6</b>	-	2	4	-	ДС+РЗ /К 2 бали
Тема 6. Захист даних від несанкціонованого доступу та пошкоджень.	<b>6</b>	-	2	4	-	ДС+РЗ /К 2 бали

Тема 7. Створення стійких паролів для PDF-документів, архівів, текстових документів.	<b>6</b>	-	2	4	-	ДС+РЗ /К 2 бали
Тема 8. Використання облікових записів для реалізації політики безпеки.	<b>6</b>	-	2	4	-	ДС+РЗ /К 2 бали
Тема 9. Налаштування захисту flash носіїв.	<b>6</b>	-	2	4	-	ДС+РЗ /К 2 бали
<b>Разом за модулем 1</b>	<b>58</b>	<b>4</b>	<b>14</b>	<b>36</b>	<b>4</b>	<b>20</b>
<b>Змістовий модуль 2. Інформаційна безпека автоматизованих систем і комунікаційних мереж</b>						
Тема 10. Шифрування даних. Загальне поняття шифрування даних. Перші шифри. Ключі шифрування. Алгоритми шифрування. Шифрування з симетричними та асиметричним ключами.	<b>6</b>	2	-	4	-	ДС+РЗ /К 2 бали
Тема 11. Шифрування тексту методом стовпцевої перестановки та подвійної перестановки	<b>7</b>	2	1	2	2	ДС+РЗ /К 4 бали
Тема 12. Використання шифру Віженера для захисту даних у MSExcel.	<b>3</b>	-	1	2	-	ДС+РЗ /К 4 бали
Тема 13. Частотний аналіз тексту за допомогою програмного продукту Wolfram Mathematica.	<b>5</b>	2	1	2	-	ДС+РЗ /К 4 бали
Тема 14. Основи безпечної роботи в мережі «Інтернет».	<b>5</b>	2	1	2	-	ДС+РЗ /К 2 бали
Тема 15. «Кібервійна та інформаційна протидія»	<b>3</b>	-	1	2	-	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	<b>3</b>	-	1	2	-	ДС+РЗ /К 2 бали
<b>Разом за модулем 2</b>	<b>32</b>	<b>8</b>	<b>6</b>	<b>16</b>	<b>4</b>	<b>20</b>
Тестування						60
<b>Всього годин/Балів</b>	<b>90</b>	<b>12</b>	<b>20</b>	<b>52</b>	<b>8</b>	<b>100</b>

\* 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
Тема 1	Поняття управління інформаційною безпекою. Основи інформаційної державної політики у сфері інформаційної безпеки.	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.
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.	4 год.
Тема 11	Криптографічний алгоритм. Основні криптографічні методології з ключем.	2 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.
Всього		52

### IV. Політика оцінювання

Оцінювання знань здобувачів освіти з ОК 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 во ВНУ 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 здобувачів 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 за дуальною формою 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 I 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 Лесі 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.](#))

## V. Підсумковий контроль

Оцінювання ОК здійснюється за 100-бальною шкалою. При вивченні ОК передбачаються такі види контролю: поточний та підсумковий. Поточний контроль здійснюється у вигляді усної відповіді на запитання під час захисту виконаних практичних робіт та тестування після вивчення змістових модулів. 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 100 балів за поточний контроль.

Якщо здобувач протягом семестру набирає необхідні бали для зарахування ОК, він може не здавати підсумковий контроль. Оцінка з ОК 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 ОК. Мінімальний бал для зарахування заліку становить 60 балів. 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. У цьому випадку всі набрані бали анулюються, і здобувач при перескладанні може отримати оцінку у діапазоні від 0 до 100 балів.

*Розподіл балів, які отримують здобувачі*

Поточний контроль			Загальна кількість балів
Змістовий модуль 1 (Т1-Т9)	Змістовий модуль 2 (Т10-16)	Тестування	
20	20	60	100

## 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 на залік

1. Поняття інформаційної безпеки та її основні складові.
2. Види інформаційних систем з точки зору захисту інформації.
3. Основні засоби протидії загрозам безпеки інформації.
4. Методи архівування та резервного копіювання даних.
5. Захист інформації від несанкціонованого доступу.
6. Частотний аналіз тексту та його практичне застосування
7. Класифікація комп'ютерних вірусів.
8. Комплексний підхід до забезпечення інформаційної безпеки в організації.
9. Ознаки зараження комп'ютера шкідливим програмним забезпеченням. Параметри безпеки та конфіденційності веббраузерів.
10. Використання Wolfram Mathematica для частотного аналізу тексту.

11. Поняття криптоаналізу та його основні методи.
12. Основні загрози під час роботи в мережі Інтернет.
13. Шифр Віженера та принцип його роботи.
14. Поняття пароля та вимоги до стійких паролів.
15. Автентифікація та авторизація користувачів.
16. Захист даних від несанкціонованого доступу та пошкоджень.
17. Методи створення та зберігання надійних паролів.
18. Захист змінних (flash) носіїв інформації.
19. Загальні поняття криптографії та шифрування даних.
20. Види захисту інформації в інформаційних системах.
21. Поняття та завдання аудиту безпеки інформаційної системи
22. Комплексна система захисту інформації (КСЗІ): структура та принципи побудови.
23. Шифрування тексту методом подвійної перестановки.

## VII. Рекомендована література

### *Основна література*

1. Браїловський М. М., Лазарєв Г. П., Хорошко В.О. Захист інформації у банківській діяльності. Київ : ТОВ “Поліграф Консалтинг”, 2004. 216 с.
2. Глинчук Л. Я. Криптологія: навч.-метод. посіб. Луцьк: Вежа-Друк, 2014. 164 с.
3. 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.
4. Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів: ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT)
5. 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.
6. Крестьянполь Л. Ю. Соціальна інженерія як засіб збору інформації. *Інформаційні технології в професійній діяльності* : зб. матеріалів І наук.-практ. семінару, 2021 р. Луцьк: ВНУ ім. Лесі Українки. С. 77–79.
7. Кузнецов О. О., Євсєєв С. П., Король О. Г. Захист інформації в інформаційних системах: навч. посіб.. Харків : ХНЕУ, 2011. 510 с.
8. 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.
9. Остапов С. Е., Євсєєв С. П., Король О. Г. Технології захисту інформації: навчальний посібник. Харків : ХНЕУ, 2013. 476 с.
10. 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>
11. Гарнавський Ю. А. Технології захисту інформації: підручник. Київ : КПІ імені Ігоря Сікорського, 2018. 162 с.
12. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. [Чинний від 28.04.1999]. Київ: ДСТСЗІ СБУ, 1999. No 22. (Нормативний документ системи технічного захисту інформації). URL: <https://tzi.com.ua/downloads/1.1-003-99.pdf>
13. Information technology. Security techniques. Information security management systems – Requirements: ISO/IEC 27001:2017.
14. Krestyanpol, L., Novachevskyi, S., & Hranovskyi, M. (2023). Application Of Blockchain Technologies For Preservation And Dissemination Of Cultural Heritage Through Nft. *Information Technology and Society*, (3 (9), 54–62. URL: <https://doi.org/10.32689/maup.it.2023.3.7>

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

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

*Методичні вказівки*

17. Крестьянполь Л. Ю. Методичні вказівки до виконання лабораторних робіт для студентів спеціальності 035 «Філологія. Прикладна лінгвістика» денної та заочної форм навчання з дисципліни "Захист інформації". Луцьк, 2021. 59 с.

*Додаткова література та інтернет-джерела*

1. Кавун С. В. Інформаційна безпека в бізнесі: наук. вид. Харків: Вид. ХНЕУ, 2007. 408 с.

2. Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України: нормативно-правова база. URL: [www.dstszi.gov.ua/dstszi/control/uk/index](http://www.dstszi.gov.ua/dstszi/control/uk/index)

3. Хорошко В. О., Чередниченко В. С., Шелест М. Є. Основи інформаційної безпеки: підручник / за ред. В. О. Хорошка. Київ : ДУІКТ, 2008. 186 с.