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 03 Гуманітарні науки

спеціальності 035 Філологія

спеціалізації 035.10 Прикладна лінгвістика

освітньо-професійної програми Прикладна лінгвістика. Переклад і комп'ютерна лінгвістика

Луцьк 2025

Силабус освітнього компонента «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.

Погоджено
Гарант освітньо-професійної програми: Калиновська І. М.

Силабус освітнього компонента затверджено на засіданні кафедри прикладної лінгвістики

протокол № 1 від 31.08.2021 р.

Завідувач кафедри: Біскуб І.П.

Силабус освітнього компонента перезатверджено на засіданні кафедри

прикладної лінгвістики протокол № 1 від 29.08.2025 р.

В. о. завідувача кафедри прикладної лінгвістики Калиновська І. М.

І. Опис освітнього компонента

Таблиця 1.1 (денна форма)

Найменування показників	Галузь знань, спеціальність, освітня програма, освітній рівень	Характеристика освітнього компонента
Денна форма здобуття освіти	**03 Гуманітарні науки 035 Філологія Прикладна лінгвістика Переклад і комп'ютерна лінгвістика Бакалавр**	**Нормативна**
		Рік навчання 4
Кількість годин/кредитів 3/90		**Семестр** 7-ий
		Лекції 10год.
		Практичні (семінарські) 22год.
		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 здобуття освіти	**03 Гуманітарні науки 035 Філологія Прикладна лінгвістика Переклад і комп'ютерна лінгвістика Бакалавр**	**Нормативна**
		Рік навчання 4
Кількість годин/кредитів 3/90		**Семестр** 7-ий
		Лекції 4год.
		Практичні (семінарські)10 год.
		Самостійна робота 64 год.
		Консультації 12 год.
		Форма контролю: екзамен
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 освітнього компонента

1. **Анотація**. ОК “Захист інформації” відноситься до циклу фахових 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 освіти. Самостійна робота ЗО в аудиторії здійснюється під час лабораторних занять, а також під час самостійного опрацювання лекційного матеріалу та підготовки до семінарів та заліку. Самостійна робота ЗО 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 курсів:
   - Інформаційні технології;
   - Основи WEB UI розробки;
   - Математичне моделювання;
   - Програмування і бази даних.
3. **Метою** викладання освітнього компонента «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 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, 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). Студенти 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.

До кінця навчання ЗО будуть компетентними з таких питань:

- володіння основними положеннями законодавства в галузі захисту інформації, міжнародних та національних стандартів безпеки інформаційних технологій (ІТ);
- Реалізація механізмів 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 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. 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 22. Застосовувати знання із логіки, технологій моделювання, експертних систем і технологій штучного інтелекту при розв'язанні задач проектування та управління інформаційними системами.

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. Класифікація загроз для інформації та їх джерел.	2	-	2	-	2	-	4	-	ДС+РЗ /К 4 бали

Класифікація основних засобів протидії загрозам безпеки.									
Тема 2. Аудит безпеки інформаційної системи.	-	2	4	2	-	-	4	2	ДС+РЗ /К 6 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 4 бали
Тема 4. Збереження цілісності інформації методами архівування.	-	2	2	2	-	2	4	-	ДС+РЗ /К 4 бали
Тема 5.Вивчення засобів захисту та зламу PDF-документів	-	2	2	-	-	-	4	2	ДС+РЗ /К 4 бали
Тема 6.Захист даних від несанкціонованого доступу та пошкоджень.	-	2	2	-	-	-	4	2	ДС+РЗ /К 4 бали
Тема 7.Створення стійких паролів для PDF-документів, архівів, текстових документів.	-	2	2	-	-	-	4	2	ДС+РЗ /К 4 бали
Тема 8. Використання облікових записів для реалізації політики безпеки.	-	2	4	-	-	-	4	2	ДС+РЗ /К 4 бали
Тема 9. Налаштування захисту flash носіїв.	-	2	4	-	-	2	4	-	ДС+РЗ /К 4 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 4 бали
Тема 11. Шифрування тексту методом	-	2	4	2	-	2	4	-	ДС+РЗ /К 4 бали

стовпцевої перестановки та подвійної перестановки									
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 6 бали
Тема 14. Основи безпечної роботи в мережі «Інтернет».	2	-	4	-	-	-	4		ДС+РЗ /К 6 бали
Тема 15. Налаштування параметрів безпеки веббраузерів.	-	2	4	-	-	-	4		ДС+РЗ /К 4 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 4 бали
Всього годин/Балів	10	22	52	6	4	10	64	12	70

*Форма контролю: ДС – дискусія, РЗ/К – розв'язування задач / кейсів.

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.	4 год.	4 год.

	Захист у базах даних та операційних системах. Заходи з моніторингу та перевірки системи управління інформаційною безпекою.		
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.	4год.	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

Політика щодо відвідування. Сам факт відвідування лекцій та практичних робіт фіксується, але не оцінюється. Оцінюється виключно робота, яку ЗО 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 вищої освіти ВНУ імені Лесі Українки.

ЗО 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 здобуття освіти у ВНУ імені Лесі Українки.

Процедура оскарження результатів контрольних заходів. ЗО 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.

Здобувачам освіти можуть бути зараховані **результати навчання, отримані у формальній, неформальній та/або інформальній освіті** В межах вивчення ОК можлива участь у конференціях, форумах, круглих столах, олімпіадах відповідного спрямування. Процес зарахування регулюється Положенням про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у ВНУ імені Лесі Українки і рішенням науково-методичної комісії факультету від 03.02.2022 року, протокол № 7.

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.

Політика щодо академічної доброчесності. Списування під час контрольних, модульних робіт та екзаменів заборонені (в т. ч. із використанням мобільних пристроїв).

Дотримання академічної доброчесності, згідно Кодексу академічної доброчесності ВНУ імені Лесі Українки, здобувачами освіти передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового
- контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується 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 порушення академічної доброчесності (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

Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти ВНУ імені Лесі Українки. оцінювання ОК «Захист інформації» здійснюється за 100-бальною шкалою.

При вивченні освітнього компоненту «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 70 балів.

Підсумковий контроль з ОК проходить у формі екзамену. Загальна кількість балів за підсумковий контроль становить 30 балів. Екзаменаційний білет включає 3 теоретичні питання, кожне з яких оцінюється у 10 балів.

Відсутність ЗО на контрольній роботі чи екзамені оцінюють у «0» балів. Повторне написання модульної чи екзаменаційної контрольної роботи та складання усного іспиту можливе лише за наявності офіційного документу, у якому зазначено поважну причину відсутності ЗО.

Рівень знань ЗО за поточний і модульний контроль оцінюють в балах і фіксують у журналі після вивчення кожного змістового модуля. Підсумкову оцінку за національною шкалою заносять в екзаменаційну відомість. Підсумковий контроль проходить у формі іспиту. Сумарна кількість балів, яку ЗО отримує при засвоєнні курсу, визначає його підсумкову оцінку, яка відповідає: відмінно / дуже добре / добре / задовільно / достатньо / незадовільно (з можливістю повторного складання).

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»).

Розподіл балів, які отримують студенти

Поточний контроль (мах 40 балів)		**Підсумковий контроль (мах 60 балів)**		**Загальна кількість балів**
Змістовий	Змістовий	Модульне	Модульне	

модуль 1 Т1-Т9	модуль 2 Т10-Т16	тестування 1	тестування 2	
35	35	15	15	100

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

Основна

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. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Людмила Ярославівна Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с
3. Information technology. Security techniques. Information security management systems – Requirements: ISO/IEC 27001:2017
4. Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів: ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT)
5. 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
6. 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.
7. Nagle F., Ransbotham S., Westerman G. The Effects of Security Management on Security Events, WEIS, 2017.
8. NIST (National Institute Of Standards And Technology). 1995. An Introduction to Computer Security: The NIST Handbook. (Special Publication 800-12).

9. 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.

10. 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.

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.

Додаткова

1. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х.: ХНЕУ, 2013. – 476 с. URL: https://www.twirpx.com/file/2340575/
2. 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.
3. Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України: нормативно-правова база. – Режим доступу: www.dstszi.gov.ua/dstszi/control/uk/index