МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет історії, політології та національної безпеки
Кафедра музеєзнавства, пам'яткознавства та інформаційно-аналітичної діяльності

СИЛАБУС
вибіркового освітнього компонента

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

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

Луцьк – 2026

Силабус освітнього компонента «ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ» підготовки бакалаврського освітнього рівня.

Розробник: Мельничук Ю. Є., доцент кафедри музеєзнавства, пам'яткознавства та інформаційно-аналітичної діяльності, к.пед.н., доцент.

Погоджено
Гарант освітньо-професійної програми: (Надольська В. В.)

Силабус освітнього компонента затверджено на засіданні кафедри музеєзнавства, пам'яткознавства та інформаційно-аналітичної діяльності

протокол № 8 від 21 січня 2026 р.

Завідувач кафедри: (Гаврилюк С. В.).

1. Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна програма, освітній рівень</th><th>Характеристика освітнього компонента</th></tr>
<tr><td>Денна форма здобуття освіти</td><td>Галузь знань
02 Культура і мистецтво</td><td>Вибірковий</td></tr>
<tr><td>Кількість годин/кредитів
150/5</td><td rowspan="2">Спеціальність
029 Інформаційна, бібліотечна та архівна справа</td><td>Рік навчання: 2-й
Семестр: 2-й</td></tr>
<tr><td rowspan="4">ІНДЗ: є</td><td>Лекції: 10 год.</td></tr>
<tr><td>Практичні (семінарські): 20 год.</td></tr>
<tr><td>Освітньо-професійна програма
«Документаційне забезпечення управління та інформаційно-аналітична діяльність»</td><td>Самостійна робота: 110 год.</td></tr>
<tr><td rowspan="2">Освітній рівень
бакалаврський</td><td>Консультації: 10 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
<tr><td colspan="2">Мова навчання українська</td><td>Навчальний план 2023 р. зі змінами 2025 р.</td></tr>
</table>

II. Інформація про викладача

ПІП: Мельничук Юлія Євгеніївна.

Науковий ступінь: кандидат педагогічних наук.

Вчене звання: доцент.

Посада: доцент кафедри музеєзнавства, пам’яткознавства та інформаційно-аналітичної діяльності.

Контактна інформація: e-mail: juliettathebest@gmail.com

Дні занять: див. електронний розклад https://ps.vnu.edu.ua/cgi-bin/timetable.cgi?n=700

III. Опис освітнього компонента

1. Анотація курсу

Навчальна дисципліна **«Технології захисту інформації»** спрямована на формування у здобувачів вищої освіти системного уявлення про принципи, методи та засоби захисту інформації в умовах цифровізації та розвитку інформаційно-комунікаційних технологій. Дисципліна орієнтована на підготовку фахівців з документознавства та інформаційно-аналітичної діяльності,

здатних забезпечувати інформаційну безпеку в процесі створення, оброблення, зберігання та використання інформаційних ресурсів і документів.

У межах курсу розглядаються основи інформаційної безпеки, загрози та ризики для інформації, методи організаційного, програмно-технічного та криптографічного захисту інформації, а також засоби контролю доступу та захисту інформаційних систем. Значна увага приділяється правовим і нормативним аспектам захисту інформації, захисту персональних даних та відповідальності за порушення вимог інформаційної безпеки.

Дисципліна охоплює питання забезпечення безпеки інформації в інформаційно-аналітичній та документно-інформаційній діяльності, формування навичок безпечної роботи з цифровими ресурсами, інформаційними системами та електронними документами. Вивчення курсу сприяє розвитку інформаційної культури, відповідального ставлення до інформації та готовності до професійної діяльності в умовах зростання інформаційних загроз.

2. Мета і завдання освітнього компонента.

Метою освітнього компонента «Технології захисту інформації» є формування у здобувачів вищої освіти системних знань про принципи, методи та засоби забезпечення захисту інформації, розвиток умінь і навичок застосування технологій інформаційної безпеки в документно-інформаційній та інформаційно-аналітичній діяльності, а також формування відповідального ставлення до збереження, оброблення та використання інформаційних ресурсів в умовах сучасного цифрового середовища.

Основними завданнями вивчення освітнього компонента є: ознайомлення здобувачів освіти з основними поняттями, принципами та складовими системи захисту інформації; формування розуміння загроз, ризиків і вразливостей інформації в інформаційних системах і документаційних процесах; вивчення організаційних, правових та нормативних засад захисту інформації; ознайомлення з методами програмно-технічного захисту інформації; формування базових знань із криптографічного захисту інформації та електронного документообігу; опанування засобів контролю доступу та управління правами користувачів; розвиток навичок безпечної роботи з інформаційними системами, цифровими ресурсами та електронними документами; формування умінь виявляти та мінімізувати інформаційні ризики в професійній діяльності; ознайомлення з вимогами щодо захисту персональних даних та конфіденційної інформації; формування інформаційної культури, професійної відповідальності та дотримання етичних норм у сфері захисту інформації.

3. Soft skills. У процесі опанування освітнього компонента «Технології захисту інформації» у здобувачів вищої освіти формуються та розвиваються такі soft skills: аналітичне та системне мислення – здатність аналізувати інформаційні загрози, ризики та вразливості; критичне мислення – уміння оцінювати надійність інформаційних систем і приймати

обґрунтовані рішення щодо захисту інформації; відповідальність та професійна доброчесність – усвідомлення наслідків порушення вимог інформаційної безпеки; інформаційна культура – дотримання правил безпечної роботи з інформаційними ресурсами та документами; цифрова грамотність – здатність ефективно й безпечно використовувати цифрові технології та інформаційні системи; уважність до деталей – вміння працювати з чутливою та конфіденційною інформацією; комунікативні навички – здатність взаємодіяти з колегами щодо питань інформаційної безпеки та захисту даних; самоорганізація та дисциплінованість – уміння дотримуватися процедур і правил інформаційної безпеки; управління ризиками – здатність прогнозувати можливі загрози та мінімізувати їх наслідки; готовність до навчання впродовж життя – прагнення постійно оновлювати знання у сфері захисту інформації.

4. Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Практ. (семін.)	Сам. роб.	Консуль-тації	Форма контролю/бали
1	2	3	4	5	6	7
Змістовий модуль 1. Основи захисту інформації та інформаційної безпеки						
Тема 1. Інформаційна безпека як складова сучасного інформаційного суспільства	7	2		5		ДС
Тема 2. Інформація як об'єкт захисту	8	2		6		ДС
Тема 3. Основні загрози та ризики інформаційній безпеці	9	2		7		ДС
Тема 4. Нормативно-правові та організаційні засади захисту інформації	10		2	7	1	ДС, УО, Р, ІРС, ІНДЗ / 6
Тема 5. Організаційні методи захисту інформації	10		2	7	1	ДС, УО, Р, ІРС, ІНДЗ / 6
Тема 6. Програмні та технічні засоби захисту інформації	10		2	7	1	ДС, УО, Р, ІРС, ІНДЗ / 6
Тема 7. Основи криптографічного захисту інформації	10		2	7	1	ДС, УО, Р, ІРС, ІНДЗ / 6
Тема 8. Захист інформації в інформаційних системах та мережах	10		2	7	1	ДС, УО, Р, ІРС / 6
Тема 9. Захист персональних даних та конфіденційної інформації	10		2	7	1	ДС, УО, Р, ІРС / 6
Разом за змістовим модулем 1	84	6	12	60	6	36 балів
Змістовий модуль 2. Технології захисту інформації в документно-інформаційній та аналітичній діяльності						
Тема 10. Захист інформації в системах електронного документообігу	11	2		8	1	ДС
Тема 11. Безпека інформаційно-аналітичних систем	11	2		8	1	ДС
Тема 12. Управління інформаційними ризиками в організаціях	11		2	9		ДС, УО, Р, ІРС / 6
Тема 13. Аудит та моніторинг інформаційної безпеки	11		2	8	1	ДС, УО, Р, ІРС / 6

Тема 14. Кіберзагрози та інциденти інформаційної безпеки	11		2	8	1	ДС, УО, Р, ІРС / 6
Тема 15. Професійна відповідальність і етика у сфері захисту інформації	11		2	9		ДС, УО, Р, ІРС / 6
Разом за змістовим модулем 2	66	4	8	50	4	24 бали
Робота на практичних заняттях						60 балів (6 балів х 10 занять)
Активна участь у роботі семінарських занять						6 балів
Відвідування і робота на лекційних заняттях						10 балів
Виконання завдань самостійної роботи						12 балів
ІНДЗ						12 балів
Усього годин/ балів	150	10	20	110	10	100 балів

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, УО – усне опитування тощо.

5. Завдання для самостійного опрацювання

Самостійна робота здобувачів вищої освіти виконується за завданням і при методичному керівництві викладача, але без його безпосередньої участі. Самостійна робота здобувачів включає як повністю самостійне освоєння окремих тем дисципліни, так й опрацювання тем, які розглядаються під час аудиторної роботи. У ході самостійної роботи здобувачі вищої освіти опрацьовують та конспектують навчальну, наукову і довідкову літературу, виконують завдання, спрямовані на закріплення знань і формування умінь та навичок, готуються до поточного і проміжного контролю з дисципліни.

№ теми	Види, зміст самостійної роботи
1	Аналіз поняття інформаційної безпеки та її ролі в сучасному інформаційному суспільстві.
2	Дослідження властивостей інформації як об'єкта захисту та класифікація видів інформації.
3	Аналіз основних загроз і ризиків інформаційній безпеці в інформаційних системах.
4	Вивчення нормативно-правових актів у сфері захисту інформації та узагальнення їх вимог.
5	Аналіз організаційних методів захисту інформації в діяльності установ та організацій.
6	Огляд програмних і технічних засобів захисту інформації та їх функціональних можливостей.
7	Вивчення основ криптографічного захисту інформації та сфери його застосування.
8	Аналіз методів забезпечення безпеки інформаційних систем і комп'ютерних мереж.
9	Дослідження особливостей захисту персональних даних і конфіденційної інформації.
10	Аналіз загроз та засобів захисту інформації в системах електронного документообігу.
11	Дослідження підходів до забезпечення безпеки інформаційно-аналітичних систем.
12	Вивчення методів управління інформаційними ризиками в організаціях.
13	Аналіз процедур аудиту та моніторингу інформаційної безпеки.
14	Дослідження типів кіберзагроз та основ реагування на інциденти інформаційної безпеки.
15	Узагальнення вимог професійної етики та відповідальності у сфері захисту інформації.

IV. Політика оцінювання

При вивченні освітнього компонента «ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ» застосовується поточний та підсумковий семестрові форми контролю. Також, передбачено обов'язковий контроль засвоєння навчального матеріалу дисципліни, віднесеного на самостійну роботу. Поточний контроль (засвоєння окремих тем) проводиться у формі усного опитування або письмового експрес-контролю на лекціях та семінарських заняттях, у формі виступів здобувачів вищої освіти з доповідями та під час дискусій при обговоренні навчальних питань на семінарських заняттях, у формі написання рефератів, виконання тематичних тестових завдань, підготовки ІНДЗ.

При вивченні освітнього компонента необхідно спиратися на конспект лекцій та рекомендовану навчальну, наукову і довідкову літературу. Вітається використання інших джерел з альтернативними поглядами на ті чи інші питання задля формування продуктивної дискусії з проблем курсу.

Відвідування занять є обов'язковим. У разі підписання здобувачем вищої освіти індивідуального плану обов'язковим є виконання індивідуальних завдань згідно зі встановленим викладачем графіком. Високо оцінюється прагнення здобувачів вищої освіти: регулярно відвідувати заняття; планомірно та систематично засвоювати навчальний матеріал; активно працювати на лекційних і семінарських заняттях, брати участь в обговоренні дискусійних питань; повною мірою долучатися до активних форм навчання; відпрацьовувати пропущені семінарські заняття. Навчання за індивідуальним графіком може бути організоване за допомогою дистанційних технологій навчання, або в інший спосіб (електронний особистий кабінет здобувача, електронна пошта, доступні аудіокомунікаційні сервіси).

Недопустимими є: пропуски з неповажних причин та запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття (окрім випадків, передбачених навчальним планом та методичними рекомендаціями викладача); списування та плагіат.

Здобувачі вищої освіти мають дотримуватися академічної доброчесності: самостійно виконувати усі навчальні завдання, завдання підсумкового контролю. У разі використання ідей, тверджень, відомостей при виконанні усіх завдань, передбачених силабусом, необхідно у формі посилань вказувати на джерела інформації. Дотримуватись норм законодавства про авторське право і суміжні права. Дотримуватись положень «Кодексу академічної доброчесності ВНУ імені Лесі Українки».

У випадку, якщо здобувач освіти не відвідував окремі аудиторні заняття з поважних причин та надав підтверджуючий документ, на консультаціях він має право відпрацювати

пропущені заняття (усно або у формі тестування) та добрати ту кількість балів, яку було визначено на пропущені теми. Пропущені з поважних причин заняття відпрацьовуються у визначений час згідно затвердженого графіка.

Консультації здобувачам вищої освіти надаються: на кафедрі згідно графіку; онлайн через Університетський портал – Office 365, за допомогою Viber чи електронної скриньки (за попередньою домовленістю з викладачем).

Результати навчання, здобуті здобувачем освіти шляхом неформальної та/або інформальної освіти, визнаються у ВНУ імені Лесі Українки шляхом валідації. Порядок та процедура визнання регламентується «Положенням про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у ВНУ імені Лесі Українки». Визнанню можуть підлягати такі результати навчання, отримані в неформальній освіті (професійні курси/тренінги, громадянська освіта, онлайносвіта, професійні стажування та ін.), які за тематикою, обсягом вивчення та змістом відповідають як освітньому компоненту в цілому, так і його окремому розділу, темі (темам), індивідуальному завданню, тощо, які передбачені силабусом навчальної дисципліни. Визнання результатів навчання, отриманих у неформальній та/або інформальній освіті, відбувається в семестрі, що передує семестру початку вивчення освітнього компонента, або під час вивчення ОК (але не пізніше початку останнього місяця навчання, враховуючи ймовірність непідтвердження здобувачем результатів такого навчання).

Загалом оцінювання здобувачів здійснюється відповідно до «Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти ВНУ імені Лесі Українки». Максимальну кількість балів (100) можна набрати упродовж семестру за результатами виконання усіх видів робіт, які передбачені силабусом:

1. Робота на практичних заняттях (максимум 60 балів – 5 балів х 12 занять).
2. Активна участь у роботі практичних занять (максимум 6 балів).
3. Відвідування і робота на лекційних заняттях (максимум 12 балів).
4. Виконання завдань самостійної роботи (максимум 10 балів).
5. Виконання ІНДЗ (максимум 12 балів).

V. Підсумковий контроль

Семестровий залік виставляється здобувачам освіти на підставі результатів виконання усіх видів запланованої навчальної роботи упродовж семестру за 100-бальною шкалою. У дату складання заліку викладач фіксує у відомості суму поточних балів, які здобувач освіти набрав під час поточної роботи (шкала від 0 до 100 балів).

У випадку, якщо здобувач освіти протягом поточної роботи набрав менше як 60 балів, він складає залік під час ліквідації академічної заборгованості. У цьому випадку бали, набрані під

час поточного оцінювання, анульовуються. Максимальна кількість балів на залік під час ліквідації академічної заборгованості – 100. Повторне складання заліку допускається не більше як два рази: один раз – викладачеві, другий – комісії, яку створює декан факультету.

Терміни проведення підсумкового семестрового контролю встановлюються графіком навчального процесу.

Перелік питань для підсумкового контролю:

Тема 1. Інформаційна безпека як складова сучасного інформаційного суспільства

1. Розкрийте сутність поняття «інформаційна безпека».
2. Обґрунтуйте значення інформаційної безпеки у професійній діяльності фахівця з документознавства.

Тема 2. Інформація як об’єкт захисту

3. Охарактеризуйте властивості інформації як об’єкта захисту.
4. Назвіть і поясніть основні види інформації, що підлягають захисту.

Тема 3. Основні загрози та ризики інформаційній безпеці

5. Назвіть основні загрози інформаційній безпеці.
6. Поясніть поняття інформаційного ризику та його складові.

Тема 4. Нормативно-правові та організаційні засади захисту інформації

7. Охарактеризуйте нормативно-правову базу захисту інформації в Україні.
8. Поясніть роль організаційних заходів у системі захисту інформації.

Тема 5. Організаційні методи захисту інформації

9. Назвіть основні організаційні методи захисту інформації.
10. Поясніть значення управління доступом та політик безпеки.

Тема 6. Програмні та технічні засоби захисту інформації

11. Охарактеризуйте програмні засоби захисту інформації.
12. Поясніть роль технічних засобів у забезпеченні інформаційної безпеки.

Тема 7. Основи криптографічного захисту інформації

13. Розкрийте сутність криптографічного захисту інформації.
14. Поясніть принципи використання електронного цифрового підпису.

Тема 8. Захист інформації в інформаційних системах та мережах

15. Охарактеризуйте основні загрози інформаційним системам і мережам.
16. Назвіть методи забезпечення безпеки інформаційних систем.

Тема 9. Захист персональних даних та конфіденційної інформації

17. Поясніть вимоги до захисту персональних даних.
18. Охарактеризуйте заходи забезпечення конфіденційності інформації.

Тема 10. Захист інформації в системах електронного документообігу

19. Назвіть загрози інформаційній безпеці в системах електронного документообігу.
20. Охарактеризуйте методи захисту електронних документів.

Тема 11. Безпека інформаційно-аналітичних систем

21. Поясніть особливості захисту інформаційно-аналітичних систем.
22. Розкрийте роль безпеки даних в аналітичній діяльності.

Тема 12. Управління інформаційними ризиками в організаціях

23. Охарактеризуйте етапи управління інформаційними ризиками.
24. Поясніть значення оцінювання ризиків для інформаційної безпеки.

Тема 13. Аудит та моніторинг інформаційної безпеки

25. Розкрийте поняття аудиту інформаційної безпеки.

26. Поясніть значення моніторингу та контролю інформаційної безпеки.

Тема 14. Кіберзагрози та інциденти інформаційної безпеки

27. Назвіть основні типи кіберзагроз.

28. Охарактеризуйте основні дії у разі виникнення інциденту інформаційної безпеки.

Тема 15. Професійна відповідальність і етика у сфері захисту інформації

29. Поясніть поняття професійної відповідальності у сфері захисту інформації.

30. Обґрунтуйте значення дотримання етичних і правових норм у професійній діяльності фахівця.

VI. Шкала оцінювання

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

VII. Рекомендована література та інтернет-ресурси

Основна література

1. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p

2. Бернакевич І.Є. Захист інформації [Електронний ресурс]. Режим доступу: http://e-learning.lnu.edu.ua/course/view.php?id=3009

3. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ.ун-т внутріш. справ, 2020. 128 с.

4. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

5. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник.– К.: Видавництво НА СБ України, 2020. – 256 с.

6. 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.

7. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації: навчальний посібник. – Х.: Новий світ-2000, 2020. – 678 с.

Додаткова література

8. Кібербезпека в сучасному світі : матеріали ІІІ Всеукраїнської науково практичної конференції (м. Одеса, 19 листопада 2021 р.) / за ред. О. В. Дикого ;уклад.: С. А. Горбаченко, Н. І. Логінова. – Одеса, 2020. – 148 с.

9. Криптоаналіз. КриптографічніІ протоколи / О.М. Гапак // Навчальний посібник з курсу «Комп'ютерна криптографія» для студентів інженерно-технічного факультету спеціальності 123-«Комп’ютерна інженерія». Ужгород: видавництво ПП «АУТДОР-ШАРК», 2021р. – 96с.

10. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.

11. Стандарти захисту персональних даних в соціальній сфері / М. В. Бем,, І. М. Городиський. –Львів: б.в., 2018. - 110 с.

12. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf