МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
вибіркового освітнього компонента
ЗАХИЩЕНІ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ
підготовки бакалавра

Луцьк – 2026

Силабус навчальної дисципліни «Захищені системи електронного документообігу» підготовки бакалавра.

Розробник: Жигаревич О.К., старший викладач

Погоджено
Гарант освітньо-професійної програми:  Чернящук Н.Л.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 6 від 15.01.2026 р.

Завідувач кафедри:  Гришанович Т. О.

І. Опис освітнього компонента

Найменування показників	**Характеристика освітнього компонента**
	Вибірковий
Денна форма навчання	Рік підготовки 2
150/5 кредитів	Семестр 4
	Лекції 10 год.
	Лабораторні 20 год.
	Самостійна робота 110 год.
ІНДЗ: немає	Консультації 10 год.
	Форма контролю: залік

ІІ. Інформація про викладача

ПІП : Жигаревич Оксана Костянтинівна
Науковий Вчене звання -
Посада старший викладач
Контактна інформація zhyharevych.oksana@vnu.edu.ua
Дні занять -

ІІІ. Опис освітнього компонента

1. **Анотація курсу.** Захищені системи електронного документообігу є одним із важливих розділів сучасних систем захисту інформації. Освітній компонент належить до переліку вибіркових навчальних дисциплін програми підготовки бакалавра за спеціальністю 125 «Кібербезпека та захист інформації», забезпечує професійний розвиток бакалавра та спрямована на формування у майбутніх фахівців базових знань, розпізнавання шкідливого програмного забезпечення в системах інформаційної та кібербезпеки; аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування та вразливостей; обирати методи зберігання та ефективні алгоритми обробки для відповідних структур даних для створення захищених програм.
2. **Мета і завдання освітнього компонента:** надання теоретичних знань та формування практичних навичок щодо організації захисту інформації з метою розв'язування прикладних задач та створення програмного забезпечення систем інформаційної безпеки.
3. **Soft skills.**

- Аналітичне та критичне мислення — здатність оцінювати ризики інформаційної безпеки, аналізувати загрози та вразливості систем електронного документообігу.
- Уважність до деталей — здатність працювати з нормативними вимогами, політиками безпеки та регламентами обробки електронних документів.
- Відповідальність та етична свідомість — усвідомлення відповідальності за збереження, цілісність і конфіденційність інформації.

- Навички прийняття обґрунтованих рішень — уміння обирати доцільні методи та засоби захисту інформації з урахуванням технічних і організаційних обмежень.
- Комунікаційні навички — здатність зрозуміло пояснювати принципи функціонування та захисту систем електронного документообігу фахівцям і нефахівцям.
- Робота в команді — ефективна взаємодія з учасниками проєктів під час розробки та впровадження захищених інформаційних систем.
- Самоорганізація та дисциплінованість — здатність дотримуватися вимог безпеки, стандартів і процедур у професійній діяльності.

4. Структура освітнього компонента.

Назви змістових модулів і тем	Усього	Лек.	Лабор.	Сам. роб.	Конс.	Форма контролю/ Бали
Змістовий модуль 1. Основи організації захисту інформації						
Тема 1. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.	12	1	2	8	1	РЗ
Тема 2. Організаційна робота із захисту інформації в країнах НАТО та ЄС.	12	1	2	8	1	РЗ
Тема 3. Вивчення міжнародного стандарту з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).	12	1	2	8	1	РЗ, РМГ
Тема 4. Вивчення організаційної роботи служби захисту інформації в автоматизованих системах.	12	1	2	8	1	РЗ
Тема 5. Технічні канали витоку інформації. Засоби технічної розвідки.	12	1	2	8	2	
Разом за модулем 1	60	5	10	40	6	**14**
Змістовий модуль 2. Організація захисту інформації в комп’ютерних системах						
Тема 1. Основні відомості прозахист інформації в комп’ютерних системах.	13	1	2	10		РЗ

Тема 2. Основи криптографічного захисту інформації.	14	1	2	10	1	РЗ
Тема 3. Організація та порядок контролю за функціонуванням системи ТЗІ в Україні.	14	1	2	10	1	РЗ
Тема 4. Загальні положення з організації якості реалізації заходів з ТЗІ.	14	1	2	10	1	РЗ
Тема 5. Основні засоби та механізми захисту інформації в комп'ютерних системах.	14	1	2	10	1	РЗ
Разом за модулем 2	50	5	10	70	4	26
Види підсумкових робіт						Бал
Тестування						25
Модульна контрольна робота						10
ІНДЗ 1						15
ІНДЗ 2						10
Всього годин/Балів	150	10	20	110	10	100

Методи контролю*: ДС – дискусія, ДБ – дебати, Т – тести, ТР – тренінг, РЗ/К – розв'язування задач/кейсів, ІНДЗ/ІРС – індивідуальне завдання/індивідуальна робота здобувача освіти, РМГ – робота в малих групах, МКР/КР – модульна контрольна робота/ контрольна робота, Р – реферат, а також аналітична записка, аналітичне есе, аналіз твору тощо.

4. Завдання для самостійного опрацювання.

Самостійна робота здобувачів включає в себе:

– Опрацювання лекційного матеріалу. Перевірка здійснюється під час практичних занять.

– Підготовка до лабораторних занять, виконання домашніх завдань.

– Перевірка здійснюється під час лабораторних занять.

– Систематизація вивченого матеріалу перед заліком. Перевірка здійснюється під час заліку.

– Вивчення тем, що не розглядаються в курсі лекцій. Перевірка здійснюється під час модульних контрольних заходів і оцінюється відповідною кількістю балів.

– Підготовка ІНДЗ. Перевірка здійснюється під час здачі індивідуального звдання.

№ з/п	Тема	Кількість годин
1	Захист компонентів операційних систем.	10
2	Безпека комп'ютерних мереж.	10
3	Сучасні технології захисту комп'ютерних мереж.	10
4	Захист інформації в мережі Internet.	10

5	Криптографічні засоби захисту інформації в комп'ютерних системах.	10
6	Принципи генерації розподілу та збереження ключів.	10
7	Криптографія в сучасних комп'ютерних технологіях.	10
8	Сертифікація засобів захисту інформації.	10
9	Порядок експлуатації управління та супроводження систем захисту інформації в захищених комп'ютерних системах.	10
10	Оцінка захищеності обчислювальної техніки.	20
11		110

IV. Політика оцінювання

Політика щодо академічної доброчесності. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно, а результати раніше зданих робіт анулюються і виконуються повторно у порядку визначеному викладачем. При цьому викладач залишає за собою право змінити завдання.

Комунікаційна політика. Здобувачі вищої освіти повинні мати активовану університетську пошту. Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту, можливе інше (додаткове) джерело комунікації, визначене викладачем для більш оперативного зв'язку зі студентами.

Політика щодо перескладання. Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).

Політика щодо оскарження оцінювання. Політика щодо оскарження оцінки. Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку згідно «Положення про порядок і процедури вирішення конфліктних ситуацій у Волинському національному університеті імені Лесі Українки»

Політика щодо відвідування занять. Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, академічна мобільність, які необхідно підтверджувати відповідними документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об'єктивних причин навчання може проводитися у дистанційній формі за погодженням з керівником курсу та деканом факультету. Декан факультету видає розпорядження про дистанційне навчання на основі заяви здобувача. Під час дистанційного навчання лабораторні роботи виконуються відповідно до розкладу занять. На початку заняття викладач повідомляє варіант завдання, який здобувач повинен виконати. Звіт про виконання лабораторної роботи необхідно завантажити в Moodle до завершення заняття. Вимоги до звітів наведені в описах лабораторних робіт у системі Moodle. Після закінчення заняття можливість здачі буде припинено. Роботи, подані несвоєчасно, не підлягають оцінюванню.

Навчання може здійснюватися за індивідуальним графіком відповідно до Положення про організацію освітнього процесу здобувачів освіти за індивідуальним графіком навчання у Волинському національному університеті імені Лесі Українки. Для цього здобувач подає заяву на ім'я декана, який, враховуючи успішність та підстави, погоджує або відхиляє

подану заяву. У разі погодження здобувач освіти погоджує із викладачем план роботи, форми та терміни контролю. Індивідуальний графік затверджується на один семестр, а під час академічної мобільності – не більше ніж на рік.

Усі умови навчання в дистанційній формі та за індивідуальним графіком також подані у дистанційному курсі цього освітнього компоненту системи Moodle.

Бонуси. Після завершення вивчення курсу та перед початком екзаменаційної сесії здобувачам вищої освіти можуть бути нараховані додаткові бали за наукову діяльність. Такі бали надаються за участь у наукових конференціях, підготовку публікацій, здобуті результати в олімпіадах чи конкурсах студентських наукових робіт та інші досягнення у предметній галузі освітнього компонента. Порядок і систему нарахування бонусних балів визначає та затверджує науково-методична комісія факультету.

Визнання результатів навчання, отриманих у формальній, неформальній освіті. Під час вивчення освітнього компонента можливе визнання результатів навчання отриманих у формальній, неформальній та/або інформальній освіті. Порядок визнання результатів навчання для здобувачів вищої освіти, набутих у: формальній освіті (академічна мобільність студентів на території України чи поза її межами, для студентів, які переводяться, поновлюються з інших ЗВО (вітчизняних чи іноземних); неформальній та/або інформальній освіті здійснюється згідно «ПОЛОЖЕННЯ про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки».

Підсумковий контроль

Форма контролю – семестровий залік. Оцінювання здійснюється за 100-бальною шкалою. Оцінка включає в себе оцінювання всіх видів запланованої навчальної роботи протягом семестру: нараховується за якісне виконання лабораторних, контрольних, тестових контрольних робіт та виконання індивідуального завдання. Максимальна кількість балів, яку може отримати здобувач під час поточного оцінювання за семестр – 100 балів. Залік виставляється за результатами поточної роботи за умови, що здобувач освіти виконав ті види навчальної роботи, які визначено силабусом освітнього компонента.

У випадку, якщо здобувач освіти не відвідував окремі аудиторні заняття (з поважних причин), на консультаціях він має право відпрацювати пропущені заняття та добрати ту кількість балів, яку було визначено на пропущені теми. У дату складання заліку викладач записує у відомість суму поточних балів, які здобувач освіти набрав під час поточної роботи.

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, становить 100. На заліку, під час ліквідації академічної заборгованості, здобувач отримує комплексне завдання, яке охоплює всі теми і всі форми контролю, які пропонувалися при вивченні освітнього компонета.

Питання, які виносяться на залік під час ліквідації академічної заборгованості

1.	Використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
2.	Побудова захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
3.	Задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом.
4.	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

5.	Вирішувати задачі управління процедурами ідентифікації, аутентифікації, авторизації процесів і користувачів згідно кібербезпеки.
6.	Забезпечення функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
7.	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
8.	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
9.	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
10.	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки.

V. 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

VI. Рекомендована література та інтернет-ресурси.

Основна література

1. Урядовий портал. Постанова Кабінету Міністрів України від 29 березня 2006 р. №373.
2. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ-2000», 2020 . – 678 с. 8. Створення та обробка баз даних: навч. посібник для студ. техн. спец. вищ. навч. закл.
3. Holistic Info-Sec for Web Developers. [Electronic resource]. – Access mode: https://holisticinfosecforwebdevelopers.com/
4. OWASP Web Security Testing Guide. [Electronic resource]. – Access mode : https://owasp.org/www-project-web-security-testing-guide/
5. Open Web Application Security Project [Електронний ресурс]. Режим доступу:
   a. www.owasp.org
6. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Практичний посібник. Київ, 2021р.370с.
7. Кіберзахист Литви: https://kam.lt/en/cyber-security

8. Місія в Україні:https://therecord.media/cyber-command-sent-a-hunt-forward-team-to-help-lithuania-harden-its-systems/
9. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології). Практичний посібник., Київ, 2022р.281с.
10. Когут Ю.І. Корпоративна безпека: практичний посібник/Ю.І.Когут. – Київ: Колсантингова компанія «СІДКОН», 2021. – 460 с.

Додаткова дітература та Інтернет-ресурси

1. Офіційний сайт Google, на якому розміщена документація по работі із Google App Engine. [Електронний ресурс]. – Режим доступу: https://cloud.google.com/products/app-engine
2. Офіційний сайт Microsoft, на якому розміщена документація по роботі із платформою Microsoft Azure. [Електронний ресурс].
3. Когут Ю.І. Кібервійна та безпека об’єктів критичної інфраструктури [практичний посібник] / Ю.І. Когут; за редакцією доктора тех., наук, проф. А.С.Довгополого. – Київ: Консалтингова компанія «СІДКОН»; ВД Дакор, 2021. – 332 с.