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

СИЛАБУС

нормативного освітнього компонента

ЦИФРОВІ ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

підготовки здобувачів освіти першого (бакалаврського) рівня
спеціальності 071 Облік і оподаткування
освітньо-професійної програми Цифровий облік та консалтинг

Луцьк – 2025

Силабус освітнього компонента «Цифрові технології інформаційної безпеки**»** підготовки здобувачів освіти першого (бакалаврського) рівня, галузі знань 07 Управління та адміністрування, спеціальності 071 Облік і оподаткування, за освітньо-професійною програмою Цифровий облік та консалтинг

Розробник: доцент, кандидат технічних наук Онищук Оксана Олександрівна

Погоджено
Гарант освітньо-професійної програми
Цифровий облік та консалтинг: Алла ФАТЕНОК-ТКАЧУК

Силабус освітнього компонента затверджено на засіданні кафедри обліку і оподаткування

протокол № 1 від 27 серпня 2025 р.

Завідувач кафедри: Тетяна Гришанович

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та **кібербезпеки**
протокол № 2 від 17 вересня 2025 р.

І. 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 rowspan="2">Денна форма здобуття освіти</td><td rowspan="8">07 Управління та адміністрування

071 Облік і оподаткування

Цифровий облік та консалтинг

Перший (бакалаврський) рівень</td><td>Нормативний</td></tr>
<tr><td>Рік навчання – 2-ий</td></tr>
<tr><td rowspan="3">Кількість годин /кредитів 90/3</td><td>Семестр – 3-ий</td></tr>
<tr><td>Лекції – 16 год.</td></tr>
<tr><td>Практичні – 10 год.
Лабораторні 10 год.</td></tr>
<tr><td rowspan="2">ІНДЗ: немає</td><td>Самостійна робота – 46 год.</td></tr>
<tr><td>Консультації – 8 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
<tr><td colspan="2">Мова навчання</td><td>Українська</td></tr>
</table>

ІІ. Інформація про викладача

ПІП – Онищук Оксана Олександрівна
Науковий ступінь – кандидат технічних наук
Вчене звання – доцент
Посада – доцент комп'ютерних наук та кібербезпеки
Контактна інформація: +38-0966943585, Onyshchuk/oksana@vnu.edu.ua

ІІІ. Опис освітнього компонента

1. Анотація ОК.

Освітній компонент є одним із базових для галузі управління та адміністрування. Безпека інформаційних систем вимагає все більшої уваги сучасного суспільства, яке все більшою мірою спирається на Інформаційні процеси (ІП), які стають рушійною силою економіки, суспільних відносин, військової справи. ІП – це процеси збору, підготовки, передачі, обробки, перетворення та використання інформації в різних сферах суспільства. Інформація, за одним із продуктивних визначень, є корисні, або ж, нові відомості про навколишній і внутрішній світ. Вона не дається нам безпосередньо, через органи відчуттів. Вона дана нам опосередковано, через фізичні носії - знаки, символи, сигнали (збурення фізичного стану середовища розповсюдження), тощо. Зазвичай їх називають даними. Предмет присвячений теоретичному викладу і отримання практичних навичок з основних тем цифрових інформаційних системах (ІС) з метою їх захисту. Даний освітній компонент сприяє розумінню та засвоєнню здобувачами багатьох аспектів функціонування інформаційних систем.

2. Пререквізити: «Основи цифрової грамотності», «Інформаційно-комунікаційні технології в галузі».

Постреквізити. «Спеціалізовані інформаційні системи в обліку», що вивчатиметься в 5-му семестрі.

3. Мета і завдання освітнього компонента.

Мета викладання освітнього компонента – набуття здобувачами знань, умінь і здатностей (компетенцій) щодо розробки та застосування методів цифрових технологій інформаційної безпеки для ефективного вирішення завдань професійної діяльності. Метою кредитних модулів є підготовка висококваліфікованих фахівців з обліку та оподаткування, які обізнані у цифрових технологіях та безпеці інформаційних систем, можуть: забезпечити конфіденційність інформації; ідентифікацію об'єктів і суб'єктів інформаційної діяльності в ІС.

4. Компетентності. Програмні результати навчання. Soft skills.

Компетентності, яких здобувач освіти набуде в результаті вивчення освітнього компонента:

Інтегральна компетентність.

Здатність розв'язувати складні спеціалізовані завдання та практичні проблеми у сфері обліку, аудиту, діджиталізації обліково-аналітичних процесів, оподаткування та консалтингу в процесі професійної діяльності, що передбачає застосування теорій та методів економічної науки і характеризується комплексністю й невизначеністю умов.

Загальні компетентності:

ЗК 01. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 08. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 15. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, вести здоровий спосіб життя.

ЗК16. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів не доброчесності.

Спеціальні (фахові) компетентності:

СК 02. Використовувати математичний інструментарій для дослідження соціально-економічних процесів, розв'язання прикладних завдань в сфері обліку, аналізу, контролю, аудиту, оподаткування.

СК 06. Здійснювати облікові процедури із застосуванням спеціалізованих інформаційних систем і комп'ютерних технологій.

СК 08. Ідентифікувати та оцінювати ризики недосягнення управлінських цілей суб'єкта господарювання, недотримання ним законодавства та регулювання діяльності, недостовірності звітності, збереження й використання його ресурсів.

Результати навчання:

ПР 04. Формувати й аналізувати фінансову, управлінську, податкову і

статистичну звітність підприємств та правильно інтерпретувати отриману інформацію для прийняття управлінських рішень.

ПР 09. Ідентифікувати та оцінювати ризики господарської діяльності підприємств.

ПР 12. Застосовувати спеціалізовані інформаційні системи і комп'ютерні технології для обліку, аналізу, контролю, аудиту та оподаткування.

ПР 17. Вміти працювати як самостійно, так і в команді, проявляти лідерські якості та відповідальність у роботі, дотримуватися етичних принципів, поважати індивідуальне та культурне різноманіття.

ПР 24. Володіти навичками застосування знань щодо систематизування інформації в спеціалізованих інформаційних системах, продуктах, сервісах і технологіях для розв'язування задач з обліку, аналізу, контролю, аудиту і оподаткування відповідно до вимог і потреб стейкхолдерів.

ПР 26. Застосовати програмні продукти та технології для забезпечення безпеки та збереження обліково-аналітичної інформації підприємства.

Soft skills.

- **Критичне мислення та аналітичні здібності.** Вміння аналізувати дані, знаходити аномалії, оцінювати ризики – особливо при роботі з інформацією, випадками порушень безпеки, змінами в законодавстві.
- **Увага до деталей.** Маленька недогляд – і можуть бути великі наслідки: помилкові звіти, витік даних, неправильне відображення показників.
- **Комунікація (усна та письмова).** Пояснювати складні технічні чи юридичні аспекти для не фахівців, готувати звіти, інструкції, спілкуватись з клієнтами чи колегами.
- **Емоційний інтелект, емпатія.** Розуміти, як інші сприймають інформацію і ризики, реагувати на зацікавлених сторін з розумінням, підтримувати хорошу командну роботу.
- **Адаптивність і гнучкість.** Технології та загрози змінюються дуже швидко (наприклад, нові види атак, зміни в законодавстві чи вимогах безпеки). Потрібно вміти швидко вчитися новим підходам, оновлювати знання й навички.
- **Самоорганізація, відповідальність та управління часом.** Робота з великим обсягом інформації, дотримання строків, багатозадачність – все це вимагає вміння планувати, пріоритезувати, бути дисциплінованим.
- **Командність та співпраця.** Часто доведеться взаємодіяти з ІТ, юридичним відділом, менеджментом, бізнес-підрозділами.
- **Етичність і професійна чесність.** Захист даних, оподаткування, фінансові звіти – все це сфері, де важлива довіра, відповідність законам, справедливість.
- **Навичка вирішувати проблеми / креативність.** Не всі загрози передбачувані; потрібна здатність мислити нестандартно, шукати нові шляхи, як реагувати на інциденти чи розробляти політики безпеки.
- **Постійне навчання / Growth mindset.** Оскільки цифрові технології, загрози і вимоги оновлюються, треба бути готовим постійно оновлювати знання – як технічні, так і галузеві (закони, стандарти безпеки, податки).

5. Структура освітнього компонента.

	Змістовні модулі	Кількість годин					
		Всього	Лек	Лаб	Прак	Конс	Сам
1	2	3	4	5	6		7
1	Змістовий модуль 1. ОСНОВНІ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ						
	Тема 1. Основні поняття і аналіз загроз інформаційної безпеки	8	1	1	1		5
	Тема 2. Проблеми інформаційної безпеки мереж	9	1	1	1	1	5
	Тема 3. Політики безпеки	10	2	1	1	1	5
	Тема 4. Стандарти інформаційної безпеки	9	2	1	1	1	4
	Тема 5. Принципи криптографічного захисту інформації	9	2	1	1	1	4
	Разом змістовий модуль1	45	8	5	5	4	23
2	Змістовий модуль 2. ЦИФРОВІ ТЕХНОЛОГІІ						
	Тема 6. Криптографічні алгоритми	10	2	1	1	1	5
	Тема 7. Технології аутентифікації	10	2	1	1	1	5
	Тема 8. Аналіз захищеності і виявлення атак	10	2	1	1	1	5
	Тема 9. Захист від вірусів	8	1	1	1	1	4
	Лекція 10. Методи управління засобами мережевої безпеки	7	1	1	1		4
	Разом змістовий модуль 2	45	8	5	5	4	23
	РАЗОМ	90	16	10	10	8	46

Форми контролю: О – опитування; ПЗ – виконання практичних завдань; ЛР – виконання лабораторної роботи

6. Завдання для самостійного опрацювання.

Самостійна робота здобувачів виконується за завданням і при

методичному керівництві викладача, але без його безпосередньої участі. Самостійна робота підрозділяється на самостійну роботу на аудиторних заняттях і на позааудиторну самостійну роботу. Самостійна робота здобувачів включає як повністю самостійне освоєння окремих тем (розділів) освітнього компонента, так і опрацювання (розділів), освоюваних під час аудиторної роботи. Під час самостійної роботи навчаються читаючи та конспектуючи навчальну, наукову та довідкову літературу, виконують завдання, спрямовані на закріплення знань і відпрацювання умінь і навичок, готуються до поточного і проміжного контролю. Організація самостійної роботи здобувачів регламентується нормативними документами, навчально-методичною літературою та електронними освітніми ресурсами.

Теми для самостійного опрацювання

№ з/п	Назва теми	Кількість годин
1	Запровадження парольної аутентифікації та розмежування доступу у програмний застосунок	6
2	Захист застосунків від несанкціонованого використання і копіювання	6
3	Використання криптографічних функцій для захисту інформації	6
4	Аналіз механізмів захисту застосунку та застосування обфускації	6
5	Автоматизований пошук вразливостей у вихідних текстах програмного забезпечення, що написані на мові високого рівня	6
6	Побудова моделі порушника та моделі загроз в інформаційній системі	6
7	Механізми безпеки баз даних	5
8	Механізми захисту операційних систем	5
РАЗОМ		46

IV. Політика оцінювання

Основні принципи організації поточного й підсумкового контролю знань здобувачів освіти розкриті у Положенні про поточне та підсумкове оцінювання знань здобувачів освіти ВНУ імені Лесі Українки від 26.06.2025 р.

Політика викладача щодо здобувача освіти.

Здобувач освіти повинен відвідувати всі заняття і брати активну участь в навчальній діяльності, а також виконувати завдання самостійної роботи. Пропущені заняття відпрацьовувати під час консультацій. Через об'єктивні причини (наприклад, хвороба, міжнародне стажування, індивідуальний план навчання, участь у наукових заходах тощо) навчання може відбуватись в онлайн формі з використанням системи Moodle, Office 365 за погодженням із керівником курсу.

Політика щодо академічної доброчесності окреслюється Положенням про систему запобігання та виявлення академічного плагіату в науковій та навчальній діяльності здобувачів вищої освіти, докторантів, науково-педагогічних і наукових працівників Волинського національного університету імені Лесі Українки від 30.01.2024 р. та Кодексом академічної доброчесності Волинського національного університету імені Лесі Українки.

Політика щодо дедлайнів та перескладання.

Терміни підсумкового контролю, ліквідації академічної заборгованості визначає розклад заліково-екзаменаційної сесії.

Можливість визнання результатів навчання, отриманих у формальній, неформальній та інформальній освіті визначається Положенням про визнання результатів, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки від 29.08.2024 р.

Можливість отримати додаткові (бонусні) бали.

Здобувачам освіти можуть бути присуджено додаткові (бонусні) бали, які зараховуються як результати поточного контролю максимум 15 балів за такі види робіт: опубліковану наукову статтю у фахових виданнях України чи рецензованих закордонних журналах – 10 балів; публікацію тез – з виступом на конференції 5 балів, без виступу – 3 бали.

V. Підсумковий контроль

Форма підсумкового семестрового контролю – залік.

Семестровий залік викладач виставляє за результатами поточної роботи за умови, що здобувач освіти виконав види навчальної роботи, запропоновані викладачем (оцінюються в діапазоні від 0 до 100 балів).

Мінімальна позитивна кількість балів – 60. Здобувач освіти може додатково скласти на консультаціях із викладачем ті теми, які він пропустив протягом семестру (з поважних причин), таким чином покращивши свій результат рівно на ту суму балів, яку було виділено на пропущені теми.

У випадку, якщо здобувач освіти набрав менше ніж 60 балів, він складає залік під час ліквідації академічної заборгованості. У цьому випадку бали, набрані під час поточного оцінювання, анулюються. Максимальна кількість балів під час ліквідації академічної заборгованості з заліку, як правило, – 100.

Залік під час ліквідацій академічної заборгованості викладач виставляє за результатами виконання завдань в письмовій формі (максимум 100 балів, з них

20 балів за кожне з двох теоретичних питань та 20 балів за розв’язання кожного з трьох практичних завдань).

Перелік питань на залік

1. Що таке інформаційна безпека та які її основні цілі?
2. Що таке загроза інформаційній безпеці? Наведіть приклади.
3. Що таке вразливість і як вона впливає на ризик?
4. Що таке ризик інформаційної безпеки та як він оцінюється?
5. Які бувають типи атак на інформаційні системи?
6. Що таке DoS-атака і як вона відрізняється від DDoS?
7. Що таке атака «людина посередині» (MITM)?
8. Що таке політика безпеки? Для чого вона потрібна?
9. Назвіть основні типи політик безпеки в організації.
10. Що таке модель доступу RBAC (Role-Based Access Control)?
11. Що таке ISO/IEC 27001 та які його основні цілі?
12. Які стандарти ІБ, крім ISO/IEC 27001, ви знаєте?
13. Яка роль аудиту інформаційної безпеки?
14. Що таке симетричне та асиметричне шифрування?
15. Що таке хеш-функція та для чого вона використовується?
16. Наведіть приклади симетричних криптоалгоритмів.
17. Як працює алгоритм RSA?
18. У чому різниця між блочним і потоковим шифруванням?
19. Що таке цифровий підпис і які його властивості?
20. Що таке аутентифікація та які є її методи?
21. Що таке двофакторна аутентифікація (2FA)?
22. Що таке сертифікат X.509 і яка його роль?
23. Що таке PKI (інфраструктура відкритих ключів)?
24. Що таке IDS та яка її функція?
25. У чому різниця між IDS і IPS?
26. Що таке вірус, троян і хробак? Наведіть приклади.
27. Які методи захисту від шкідливого ПЗ ви знаєте?
28. Що таке міжмережевий екран (firewall) і які бувають його типи?
29. Що таке VPN і як він забезпечує безпеку?
30. Що таке DMZ у мережевій архітектурі?

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

1. Lehenchuk, S.F., Vygivska, I.M., & Hryhorevska, O.O. (2022). **Protection of accounting information in the conditions of cyber security**. *Problems of Theory and Methodology of Accounting, Control and Analysis*, № 2(52), 40-46. ouci.dntb.gov.ua

2. Zhydovska, N., Drozdova, O., & Fursa, T. (2024). **The use of multi-factor authentication to ensure the security of accounting in the era of the digital economy of Ukraine**. *Economics. Finances. Law*, 2024, № -, 16-22. ouci.dntb.gov.ua

3. Skrypnyk, M., & Hryhorevska, O. (2020). **Organization of accounting information protection in terms of cyber security**. *Scientific Notes of Ostroh Academy National University, Economy Series*, No. 19(47), 95-102. journals.oa.edu.ua

4. Dorosh, Iryna. (2023). **Cyber security and its role in the financial sector: threats and protection measures**. *Economics. Finances. Law*, № 10, 2023. efp.in.ua

5. Savkiv, U.S., & Kuzmin, T.L. (2023). **Improving Accounting and Reporting in the Digital Economy**. *The Actual Problems of Regional Economy Development*, 2(19), 87-95. journals.pnu.edu.ua

6. Two-factor authentication (2FA). Електронний ресурс. Режим доступу: https://searchsecurity.techtarget.com/definition/two-factor-authentication .

7. Registry Key Security and Access Rights. Електронний ресурс. Режим доступу: https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-key-security-and-access-rights

8. Cryptography Hash functions. Електронний ресурс. Режим доступу: https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm.

9. Microsoft Cryptographic Service Providers. Електронний ресурс. Режим доступу: https://docs.microsoft.com/en-us/windows/win32/seccrypto/microsoft-cryptographic-service-providers

10. Block Ciphers Modes of Operation. Електронний ресурс. Режим доступу: http://www.crypto-it.net/eng/theory/modes-of-block-ciphers.html .

11. Haahr M. Pseudo-Random Number Generators (PRNGs). Електронний ресурс. Режим доступу: https://www.random.org/randomness/ .

12. Cryptographic Generators. Електронний ресурс. Режим доступу: https://people.seas.harvard.edu/~salil/pseudorandomness/prgs.pdf .

13. Dewhurst R. Static Code Analysis. Електронний ресурс. Режим доступу: https://owasp.org/www-community/controls/Static_Code_Analysis .