

Міністерство освіти і науки України
Сумський національний аграрний університет
Факультет економіки і менеджменту
Кафедра обліку і оподаткування

Робоча програма (силабус) освітнього компонента
Інформаційна безпека та захист даних

Реалізується в межах освітньої програми «Облік і оподаткування»
за спеціальністю D1 «Облік і оподаткування»
на другому (магістерському) рівні вищої освіти

Розробник: 4 Сергій ГАРКУША, к.е.н., доцент, доцент кафедри обліку і оподаткування

Розглянуто,
схвалено та протокол від 11.06.2026 р. №16
затверджено на
засіданні кафедри
обліку і
оподаткування

Завідувач
кафедри

Інна НАЗАРЕНКО

Погоджено:

Гарант освітньої програми

Інна НАЗАРЕНКО

Декан факультету,
де реалізується освітня
програма

Світлана ЛУКАШ

Рецензія на робочу програму
(додається) надана:

Інна НАЗАРЕНКО

Микола ГОРДІЄНКО

Методист відділу якості освіти,
ліцензування та акредитації

4. Гар
(підпис)

(Надія Баранік)

Зареєстровано в електронній базі: дата: 15.06. 2026 р.

1. ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ОСВІТНІЙ КОМПОНЕНТ

1.	Назва ОК	Інформаційна безпека та захист даних							
2.	Факультет/кафедра	Економіки і менеджменту/Обліку і оподаткування							
3.	Статус ОК	Вибірковий							
4.	Програма/Спеціальність (програми), складовою яких є ОК для								
5.	ОК може бути запропонований для	Облік і оподаткування							
6.	Рівень НРК	7							
7.	Семестр та тривалість вивчення	Для денної форми: 3 семестр, 12 тижнів. Для заочної форми: 3 семестр							
8.	Кількість кредитів ЄКТС	Обсяг навчальної дисципліни становить 5 кредитів ЄКТС – денна форма навчання. Обсяг навчальної дисципліни становить 5 кредитів ЄКТС – заочна форма навчання.							
9.	Загальний обсяг годин та їх розподіл	денна форма				заочна форма			
		Контактна робота (заняття)			Самостійна робота	Контактна робота (заняття)			Самостійна робота
		Лекційні	Практичні /семінарські	Лабораторні		Лекційні	Практичні /семінарські	Лабораторні	
		24	24	-	102	8	8	-	134
10.	Мова навчання	українська							
11.	Викладач/Координатор освітнього компонента	к.е.н., доцент Гаркуша Сергій Анатолійович							
11.1	Контактна інформація	м. Суми, вул. Г. Кондратьєва, 160, факультет Економіки і менеджменту, кафедра Обліку і оподаткування (ауд. 109е), serhii.harkusha@snau.edu.ua							
12.	Загальний опис освітнього компонента	Освітній компонент «Інформаційна безпека та захист даних» спрямований на формування у здобувачів вищої освіти системи знань, умінь і практичних навичок у сфері забезпечення захисту інформації в сучасних інформаційно-комунікаційних системах. Дисципліна охоплює теоретичні та прикладні аспекти інформаційної безпеки, включаючи моделі та принципи захисту інформації, управління ризиками, а також організаційно-правові засади захисту персональних даних. У межах освітнього компонента розглядаються можливі загрози інформаційній безпеці, методи їх виявлення та нейтралізації, засоби апаратного і програмного захисту інформації, основи криптографічного захисту даних, а також особливості забезпечення безпеки комп'ютерних мереж і глобальних інформаційних ресурсів. Значна увага приділяється практичним аспектам застосування антивірусного програмного забезпечення, засобів захисту вебсередовищ, технологій електронного цифрового підпису та захищеного електронного документообігу. Освітній компонент формує компетентності щодо аналізу та оцінювання інформаційних ризиків, вибору та застосування сучасних засобів захисту інформації, а також забезпечення конфіденційності, цілісності та доступності даних в умовах цифрової трансформації суспільства та зростання кіберзагроз							
13.	Мета освітнього компонента	Формування у здобувачів вищої освіти знань щодо теоретичних і практичних аспектів інформаційної безпеки, захисту інформаційних ресурсів та персональних даних, використання сучасних технологій і засобів захисту інформації в інформаційно-комунікаційних системах, а також набуття навичок забезпечення безпеки облікової							

		інформації, попередження інформаційних ризиків і шахрайства в умовах цифрової трансформації діяльності суб'єктів господарювання
14.	Передумови вивчення ОК, зв'язок з іншими освітніми компонентами ОП	передумови відсутні
15.	Політика академічної доброчесності	Політика академічної доброчесності передбачає самостійне виконання здобувачами освіти всіх видів навчальних завдань, дотримання встановлених строків та порядку подання робіт, недопущення академічного плагіату, фабрикації, фальсифікації, списування та інших проявів академічної недоброчесності. Під час підготовки письмових робіт обов'язковим є коректне цитування використаних джерел із належним оформленням посилань. Використання інструментів штучного інтелекту допускається виключно як допоміжного засобу для пошуку інформації, аналізу даних, перевірки текстів та генерації ідей за умови критичного опрацювання отриманих результатів здобувачем освіти. Забороняється подавати результати, повністю створені засобами штучного інтелекту, як власну авторську роботу без належного зазначення факту їх використання. За порушення принципів академічної доброчесності до здобувачів освіти можуть застосовуватися заходи академічної відповідальності відповідно до внутрішніх нормативних документів закладу вищої освіти. Документи стосовно академічної доброчесності наведені на сторінці сайту: https://snau.edu.ua/pro-universitet/struktura-universitetu/viddil-jakosti-osviti-licenzuvannja-ta-akreditacii/zabezpechennja-jakosti-osviti/akademichna-dobrochesnist/
16.	Посилання на Moodle	https://cdn.snau.edu.ua/moodle/course/view.php?id=5305
17.	Ключові слова	Інформаційна безпека, персональні дані, апаратні засоби захисту, програмні загрози, шкідливе програмне забезпечення, криптографічний захист, безпека, автоматизовані системи обліку

2. РЕЗУЛЬТАТИ НАВЧАННЯ ЗА ОСВІТНІМ КОМПОНЕНТОМ ТА ЇХ ЗВ'ЯЗОК З ПРОГРАМНИМИ РЕЗУЛЬТАТАМИ НАВЧАННЯ

Результати навчання за ОК: Після вивчення освітнього компонента студент очікувано буде здатен...»	Як оцінюється РНД
ДРН 1. Здатність до розмежування існуючих підходів до визначення поняття політика інформаційної безпеки.	Виконання завдань, експрес-опитування, тестування й обробка результатів
ДРН 2. Володіти правилами безпеки при роботі із комп'ютерними мережами	Виконання завдань, експрес-опитування, тестування й обробка результатів
ДРН 3. Аналізувати криптографічні методи захисту інформації	Виконання завдань, експрес-опитування, тестування й обробка результатів
ДРН 4. Аналізувати загрози, пов'язані з використанням шкідливого програмного забезпечення, та оцінювати ризики для інформаційних систем	Виконання завдань, експрес-опитування, тестування й обробка результатів
ДРН 5. Оцінювати рівень безпеки використання ресурсів WWW із застосуванням антивірусних програм та захисних функцій web-браузерів	Виконання завдань, експрес-опитування, тестування й обробка результатів
ДРН 6. Вміти розробляти й вирішувати актуальні питання теорії і практики інформаційної безпеки	Виконання завдань, експрес-опитування, тестування й обробка результатів

3. ЗМІСТ ОСВІТНЬОГО КОМПОНЕНТА (ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ)

Тема. Перелік питань, що будуть розглянуті в межах теми	Розподіл в межах загального бюджету часу (денна/заочна)			Рекомендована література	
	Аудиторна робота				Самостійна робота
	Лк	П.з / семін. з	Лаб . з.		
Тема 1. Теоретичні основи інформаційної безпеки. Поняття інформаційної безпеки. Основні складові інформаційної безпеки. Важливість і складність проблеми інформаційної безпеки. Концепція керування безпекою інформаційних технологій. Елементи безпеки. Процес керування безпекою інформаційних технологій. Моделі інформаційної безпеки. Архітектура інформаційної безпеки. Аналіз моделей моніторингу.	2/2	2/2		16/20	Основні джерела: 1, 2, 4, 5, 6, 7; 8; 9 Додаткові джерела: 1, 5, 6, 7, 8, 9, 10,11, 13, 14; Програмне забезпечення: -
Тема 2. Інформаційна система персональних даних. Суб'єкти відносин, пов'язаних із персональними даними. Об'єкти захисту. Загальні вимоги до обробки персональних даних. Особливі вимоги до обробки персональних даних. Права суб'єкта персональних даних. Повідомлення про обробку персональних даних. Використання персональних даних. Підстави для обробки персональних даних. Збирання персональних даних. Порядок доступу до персональних даних. Відстрочення або відмова у доступі до персональних даних. Забезпечення захисту персональних даних.	2/2	2/2		16/16	Основні джерела: 1, 2, 3, 4, 5, 6, 7; 8; 9 Додаткові джерела: 1, 5, 6, 7, 8, 9, 10, 11, 12, 13; Програмне забезпечення: -
Тема 3. Апаратні засоби захисту інформації.	4/-	4/-		14/20	Основні джерела: 1, 2, 3, 4, 5, 6, 7; 8; 9

Основи апаратного захисту. Класифікація технічних засобів зняття інформації. Основні групи технічних засобів ведення розвідки. Радіомікрофони. Основні методи прослуховування телефонних ліній. Телефонні радіо транслятори. Системи прослуховування повідомлень. Використання телефонної лінії для прослуховування приміщень. Спеціальні пристрої прослуховування. Системи і пристрої відео контролю. Пристрої дистанційного управління, відеодетектор руху. Системи та засоби виявлення, пошуку та знешкоджування технічних засобів зняття інформації. Основні стаціонарні засоби захисту інформації. Пошукове устаткування.					Додаткові джерела: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12; Програмне забезпечення: -
Тема 4. Програмні засоби, що містять небезпеку. Основні означення і критерії загроз. Найпоширеніші загрози доступності. Деякі приклади загроз доступності. Шкідливе програмне забезпечення. Основні загрози цілісності. Основні загрози конфіденційності.	4/-	4/-		14/22	Основні джерела: 1, 2, 3, 4, 5, 6, 7; 8; 9 Додаткові джерела: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12; Програмне забезпечення: -
Тема 5. Криптографічний захист інформації. Криптографічні методи захисту. Основи крипто аналізу. Стеганографія.	4/-	4/-		14/20	Основні джерела: 1, 2, 3, 4, 5, 6, 7; 8; 9 Додаткові джерела: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12; Програмне забезпечення: 2, 3, 4, 5, 6
Тема 6. Безпека в комп'ютерних мережах. Короткі відомості про комп'ютерні мережі. Використання міжмережевих екранів. Політика безпеки під час роботи в мережі. Архівування та зберігання облікової інформації. Захист інформації та попередження шахрайства у сфері	4/2	4/2		14/16	Основні джерела: 1, 2, 3, 4, 5, 6, 7; 8; 9 Додаткові джерела: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12; Програмне забезпечення: 1

облікового забезпечення					
Тема 7. Захист інформації в глобальних мережах. Короткі відомості про глобальні комп'ютерні мережі. Характер проведення атак у глобальних мережах. Захист під час використання WWW (WorldWideWeb). Захист електронних листів та поштових систем	4/2	4/2		14/20	Основні джерела: 1, 2, 3, 4, 5, 6, 7; 8; 9 Додаткові джерела: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12; Програмне забезпечення: -
Всього	24/8	24/8		102/134	

4. МЕТОДИ ВИКЛАДАННЯ ТА НАВЧАННЯ

ДРН	Методи викладання (робота, що буде проведена викладачем <u>під час аудиторних занять, консультацій</u>)	Методи навчання (які види навчальної діяльності має виконати <u>студент самостійно</u>)
ДРН 1. Здатність до розмежування існуючих підходів до визначення поняття політика інформаційної безпеки.	Словесні: монологічні (пояснення, лекція); діалогові (бесіда). Наочні: демонстрація (мультимедійний файл)	Дослідницький метод (здобувачі освіти самостійно працюють під час засвоєння знань: аналізують явища, формують проблеми, висувають і перевіряють гіпотези, самостійно формують висновки)
ДРН 2. Володіти правилами безпеки при роботі із комп'ютерними мережами	Словесні: монологічні (пояснення, лекція); діалогові (бесіда). Наочні: демонстрація (мультимедійний файл); спостереження (технологія, операція)	Дослідницький метод (здобувачі освіти самостійно працюють під час засвоєння знань: аналізують явища, формують проблеми, висувають і перевіряють гіпотези, самостійно формують висновки)
ДРН 3. Аналізувати криптографічні методи захисту інформації	Словесні: монологічні (пояснення, лекція); діалогові (бесіда). Наочні: демонстрація (мультимедійний файл); спостереження (технологія, операція)	Дослідницький метод (здобувачі освіти самостійно працюють під час засвоєння знань: аналізують явища, формують проблеми, висувають і перевіряють гіпотези, самостійно формують висновки)
ДРН 4. Аналізувати загрози, пов'язані з використанням шкідливого програмного забезпечення, та оцінювати ризики для інформаційних систем	Словесні: монологічні (пояснення, лекція); діалогові (бесіда). Наочні: демонстрація (мультимедійний файл); спостереження (технологія, операція)	Дослідницький метод (здобувачі освіти самостійно працюють під час засвоєння знань: аналізують явища, формують проблеми, висувають і перевіряють гіпотези, самостійно формують висновки)
ДРН 5. Оцінювати рівень	Словесні: монологічні	Дослідницький метод

безпеки використання ресурсів WWW із застосуванням антивірусних програм та захисних функцій web-браузерів.	(пояснення, лекція); діалогові (бесіда). Наочні: демонстрація (мультимедійний файл); спостереження (технологія, операція)	(здобувачі освіти самостійно працюють під час засвоєння знань: аналізують явища, формують проблеми, висувують і перевіряють гіпотези, самостійно формують висновки)
ДРН 6. Вміти розробляти й вирішувати актуальні питання теорії і практики інформаційної безпеки	Словесні: монологічні (пояснення, лекція); діалогові (бесіда). Наочні: демонстрація (мультимедійний файл); спостереження (технологія, операція)	Дослідницький метод (здобувачі освіти самостійно працюють під час засвоєння знань: аналізують явища, формують проблеми, висувують і перевіряють гіпотези, самостійно формують висновки)

5. ОЦІНЮВАННЯ ЗА ОСВІТНІМ КОМПОНЕНТОМ

5.1. Діагностичне оцінювання (зазначається за потреби)

5.2. Сумативне оцінювання

5.2.1. Для оцінювання очікуваних результатів навчання¹

здобувачів денної форми навчання передбачено

№	Методи сумативного оцінювання	Бали / Вага у загальній оцінці	Дата складання
1.	Дискусії	10 / 10%	Кожного практичного заняття
2.	Виконання завдань	60 / 60%	Кожного практичного заняття
3.	Експрес-опитування	20 / 20%	Кожного практичного заняття
4.	Стандартизовані тести	10 / 10%	Кожного практичного заняття

Для оцінювання очікуваних результатів навчання здобувачів заочної форми навчання передбачено

№	Методи сумативного оцінювання	Бали / Вага у загальній оцінці	Дата складання
1.	Виконання завдань	50 / 50%	Кожного практичного заняття
2.	Експрес-опитування	20 / 20%	Кожного практичного заняття
3.	Тест множинного вибору	30 балів / 30%	Відповідно до графіку освітнього процесу

5.2.2. Критерії оцінювання для здобувачів денної форми навчання

Компонент	Незадовільно	Задовільно	Добре	Відмінно
Дискусії	0-3 балів Пасивна участь у дискусії	4-6 балів Участь у дискусії, необгрунтовані відповіді	7-8 балів Активна участь у дискусії, продемонстровано навички критичного мислення	9-10 балів Активна участь у дискусії, продемонстровано навички критичного мислення, системність знань та креативність
Виконання завдань	<35 балів Завдання не виконано	36-44 балів Завдання виконане, але деякі питання не розкриті, мають місце неточності	45-53 балів Завдання виконане, але мають місце незначні неточності	54-60 балів Завдання виконане, всі питання розкриті
Експрес-опитування	0-11 балів Відсутні знання по теоретичним питанням	12-14 балів Низький рівень знань теоретичних питань	15-17 балів Володіння понятійно-категоріальним апаратом, фаховою термінологією, теоретичними знаннями, незначні неточності у відповідях на питання	18-20 балів Володіння понятійно-категоріальним апаратом, фаховою термінологією, теоретичними знаннями
Стандартизовані тести	0-5 балів Вірно вирішено менше 60 % тестів	6 балів Вірно вирішено 60 -74 % тестів	7-8 балів Вірно вирішено 75 - 89 % тестів	9-10 балів Вірно вирішено 90 і більше % тестів

¹Здобувачі вищої освіти мають право на перерахування результатів навчання набутих у неформальній/інформальній освіті відповідно до Положення про порядок визнання результатів, здобутих шляхом неформальної та/або інформальної освіти (<http://surl.li/ummbf>)

Критерії оцінювання для здобувачів заочної форми навчання

Компонент	Незадовільно	Задовільно	Добре	Відмінно
Виконання завдань	<i><29 балів</i>	<i>30-36 балів</i>	<i>37-44 балів</i>	<i>45-50 балів</i>
	Завдання не виконано	Завдання виконане, але деякі питання не розкриті, мають місце неточності	Завдання виконане, але мають місце незначні неточності	Завдання виконане, всі питання розкриті
Експрес-опитування	<i>0-11 балів</i>	<i>12-14 балів</i>	<i>15-17 балів</i>	<i>18-20 балів</i>
	Відсутні знання по теоретичним питанням	Низький рівень знань теоретичних питань	Володіння понятійно-категоріальним апаратом, фаховою термінологією, теоретичними знаннями, незначні неточності у відповідях на питання	Володіння понятійно-категоріальним апаратом, фаховою термінологією, теоретичними знаннями
Тест множинного вибору	<i>0-17 балів</i>	<i>18-21 балів</i>	<i>22-26 балів</i>	<i>27-30 балів</i>
	Вірно вирішено менше 60 % тестів	Вірно вирішено 60 -74 % тестів	Вірно вирішено 75 - 89 % тестів	Вірно вирішено 90 і більше % тестів

5.3. Формативне оцінювання:

Для оцінювання поточного прогресу у навчанні та розуміння напрямів подальшого удосконалення передбачено

№	Елементи формативного оцінювання	Дата
1	Настанови викладача в процесі виконання завдань	Кожного практичного заняття
2	Усне опитування	Кожного практичного заняття
3	Спостереження за ходом вирішення завдань, обговорення та усні коментарі викладача	Кожного практичного заняття
4	Контроль за виконанням завдань	Кожного практичного заняття
5	Перевірка тестів і обговорення результатів тестування	На наступну пару після проведення тестування

6. НАВЧАЛЬНІ РЕСУРСИ (ЛІТЕРАТУРА)

6.1. Основні джерела

6.1.1. Підручники, посібники

1. Електронна бухгалтерія: підручник. 2-е вид., перер. та допов. В.Я. Плаксієнко, І.М. Назаренко, С.А. Гаркуша, К.С. Жадько, О.В. Назаренко / За ред. В.Я. Плаксієнка. Київ: Вид-во «SBA Print», 2026. 312 с.
2. Пашорін В.І. Безпека інформаційних систем : навч. посіб. / В. І. Пашорін, Ю. В. Костюк. Київ : Держ. торг.-екон. ун-т, 2023. 376 с. URL: <https://files.znu.edu.ua/files/Bibliobooks/Inshi85/0064775.pdf>
3. Сілін Є.С., Кадубовський О.А. Основи кібербезпеки: навчальний посібник. Дніпро. 2023. 200с. URL: https://www.researchgate.net/publication/392285211_Osnovi_kiberbezpeki_navcalnij_posibnik
4. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. Кропивницький: ЦНТУ, 2022. 967 с. URL: <https://dspace.kntu.kr.ua/server/api/core/bitstreams/4ddb7930-df8e-469e-b44d-a4be9c2f15f6/content>
5. Тарнавський Ю.А. Безпека інформаційних систем : підручник. КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2023. 161 с. URL: <https://ela.kpi.ua/server/api/core/bitstreams/71eb3ad4-103b-494a-b80e-d58a49033cd5/content>

6.1.2. Методичне забезпечення

6. Методичний комплекс «Інформаційна безпека та захист даних» в програмі MOODLE. URL :<https://cdn.snau.edu.ua/moodle/course/view.php?id=5475>
7. Інформаційна безпека та захист даних : конспект лекцій для здобувачів вищої освіти освітніх програм галузей знань 05 «Соціальні та поведінкові науки» (С «Соціальні науки, журналістика та інформація»); 07 «Управління та адміністрування», 28 «Публічне управління та адміністрування» (Д «Бізнес, адміністрування та право»); 12 «Інформаційні технології» (Ф «Інформаційні технології») денної та заочної форм навчання другого (магістерського) рівня / укл.: С.А. Гаркуша. - Суми, 2024. – 102 с.
8. Інформаційна безпека та захист даних : методичні рекомендації щодо проведення практичних занять для здобувачів вищої освіти освітніх програм галузей знань 05 «Соціальні та поведінкові науки» (С «Соціальні науки, журналістика та інформація»); 07 «Управління та адміністрування», 28 «Публічне управління та адміністрування» (Д «Бізнес, адміністрування та право»); 12 «Інформаційні технології» (Ф «Інформаційні технології») денної та заочної форм навчання другого (магістерського) рівня / укл.: С.А. Гаркуша. - Суми, 2024. – 54 с.
9. Інформаційна безпека та захист даних : методичні рекомендації для самостійної роботи для здобувачів вищої освіти освітніх програм галузей знань 05 «Соціальні та поведінкові науки» (С «Соціальні науки, журналістика та інформація»); 07 «Управління та адміністрування», 28 «Публічне управління та адміністрування» (Д «Бізнес, адміністрування та право»); 12 «Інформаційні технології» (Ф «Інформаційні технології») денної та заочної форм навчання другого (магістерського) рівня / укл.: С.А. Гаркуша. - Суми, 2024. – 60 с.

6.2. Додаткові джерела

1. Гаркуша С. Кризові ризики бізнесу та автоматизація обліку: сучасні виклики і перспективи. *Стратегічні пріоритети розвитку бухгалтерського обліку, аудиту та оподаткування в умовах глобалізації* : матеріали IV Міжнародної науково-практичної конференції (м. Суми, 18 листопада 2025 р.) / за ред. проф. Назаренка О.В. Суми: СНАУ, 2025. С. 25-27. URL: https://repo.snau.edu.ua/bitstream/123456789/15377/1/36ірник_МНПК_СНАУ%2018.11.2025.pdf
2. Гаркуша С.А. Діджиталізація обліково-управлінських процесів. *Сучасний стан та перспективи економічного розвитку України: теорія, методологія, практика* :

колективна монографія / Кол. авторів. Полтава: ПП «Астроя», 2023. С. 95-104. URL: <http://www.economics.in.ua/2023/04/collectivemonograph.html>

3. Гаркуша С.А. Захист бухгалтерської інформації в автоматизованих системах обліку. *Браславські читання. Економіка XXI століття: національний та глобальний виміри: Збірник матеріалів II Міжнародної наукової-практичної конференції, 06 листопада 2024 року*. Одеса, ОДАУ. 2024. С. 353-355

4. Гаркуша С.А. Організація захисту бухгалтерської інформації в автоматизованих системах обліку. *Економіка та суспільство*. 2024. Випуск 67. DOI: <https://doi.org/10.32782/2524-0072/2024-67-26>

5. Йона Л.Г., Онацький О.В., Белова Ю.В. Криптографічний захист інформації: навч. посіб. Одеса, 2023. 200 с. URL: <https://dspace.onua.edu.ua/server/api/core/bitstreams/eeff6a3b-4b9d-40f8-ab8b-7485017ff737/content>

6. Котенко А.М., Туровський О.Л., Шуклін Г.В., Пепа Ю.В., Іванченко І.С., Аверічев І.М. Компонентна база засобів кібербезпеки та захисту інформації: Навчальний посібник. 2025. К.: ДУІКТ. 236 с. URL: https://duikt.edu.ua/uploads/1_2376_40131646.pdf

7. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с. URL: https://dspace.nau.edu.ua/bitstream/NAU/57731/1/Інформаційна%20безпека_курс%20лекцій_2022.pdf

8. Пірог О.В. Безпека вебдодатків : навч. посібн. Житомир : Житомирська політехніка, 2025. 290 с. URL: <https://surl.li/sbgwxv>

9. Про захист персональних даних: Закон України від 01.06.2010 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

10. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства: монографія / Н. Уханова; за заг. ред. В. Пилипчука. КиївОдеса: Фенікс, 2022. 140 с. URL: <http://ippi.org.ua/problemi-protidii-negativniminformatsiiniim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus>

11. Управління мережевою безпекою : конспект лекцій. Чернігів : НУ «Чернігівська політехніка», 2025. 105 с. URL: <https://ir.stu.cn.ua/server/api/core/bitstreams/f3e822f0-0c12-48ab-9707-c99c4d776208/content>

12. Усік П.С., Буравченко К.О. Безпека банківських систем : навч. посіб. / П. С. Усік, К. О. Буравченко; М-во освіти і науки України, Центральноукр. нац. техн. ун-т. Кропивницький: ЦНТУ, 2022. 194 с. URL: <https://dspace.kntu.kr.ua/server/api/core/bitstreams/29a2e041-c31e-44d9-b074-a26dfddfa97d/content>

13. Harkusha S. Information protection in automated accounting systems: user aspect. *Anti-Crisis Strategy for the Development of Socio-Economic Systems: Global Challenges: Collective monograph*. Riga, Latvia: Baltija Publishing, 2024. pp.266-291. DOI: <https://doi.org/10.30525/978-9934-26-500-6-12>

14. OSINT Open Source Intelligence. Інструменти та методи: навчальний посібник / Користін О., Демедюк С., Ісмайлов К., Ланде Д. та ін., за заг. ред. Користіна О.Є., Демедюка С.В. Київ: 7БЦ, 2025. 460 с. URL: <https://dspace.oduvs.edu.ua/server/api/core/bitstreams/3de653ea-d09e-469a-8e25-1cfaa3c84dfd/content>

6.3. Програмне забезпечення

1. ВАС Бухгалтерія.
2. Дія.Підпис – сервіс створення та використання електронного підпису.
3. [Центральний засвідчувальний орган України](#) – перевірка сертифікатів та електронних підписів.
4. [Інтегрована система електронної ідентифікації ID.GOV.UA](#) – використання КЕП для автентифікації користувачів.

5. [КНЕДП ДПС України](#) – отримання та використання кваліфікованих сертифікатів відкритих ключів.
6. Вчасно.КЕП – сервіс підписання електронних документів.