**ПрАТ "ВНЗ "МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ"**

**Інститут безпеки**

МАУП

Кафедра інформаційної та фінансової безпеки

Затверджую:
Директор Інституту безпеки
_____
Сергій ЛИСЕНКО
"06" серпня 2025 р.

Схвалено на засіданні кафедри
інформаційної та фінансової безпеки
Протокол № 1 від 06 серпня 2025 р.
Зав. кафедри
_____
Сергій ЛИСЕНКО

# *СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ»*

Спеціальності: **К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)**
**F5 Кібербезпека та захист інформації**

Освітнього рівня: **перший (бакалаврський) рівень**

Освітньої програми: **«Національна безпека (за окремими сферами забезпечення і видами діяльності)»**

Спеціалізація: _____

Київ МАУП 2025

**Розробник силабусу навчальної дисципліни:**

***Веклич Владислав Олександрович*** *- доктор юридичних наук, професор кафедри інформаційної та фінансової безпеки*

ВВО

*(підпис)*

**Викладач:**

***Веклич Владислав Олександрович*** *- доктор юридичних наук, професор кафедри інформаційної та фінансової безпеки*

ВВО

*(підпис)*

Силабус розглянуто на засіданні кафедри інформаційної та фінансової безпеки

Протокол № 1 від «06» серпня 2025р.

**Загальна інформація про навчальну дисципліну**

| | |
|---|---|
| Назва навчальної дисципліни | **Теоретичні основи захисту інформації** |
| Шифр та назва спеціальності | К3 Національна безпека (за окремими сферами забезпечення і видами діяльності) |
| Рівень вищої освіти | перший (бакалаврський) рівень |
| Статус дисципліни | обов'язкова |
| Кількість кредитів і годин | **6 кредитів/180 год**<br>Лекції : **30**<br>Семінарські заняття:**40**<br>Самостійна робота студентів: **110** |
| Терміни вивчення дисципліни | III семестр |
| Мова викладання | українська |
| Вид підсумкового контролю | **екзамен** |
| Сторінка дисципліни на сайті | https://maup.com.ua/assets/files/kafedra/nacbezpeka/sylabus-b/vstup-do-specialnosti-nacionalna-bezpeka.pdf |

**Загальна інформація про викладача. Контактна інформація.**

| ***Веклич Владислав Олександрович*** | |
|---|---|
| **Науковий ступінь** | доктор юридичних наук |
| **Вчене звання** | доцент |
| **Посада** | професор кафедри інформаційної та фінансової безпеки |
| **Дисципліни, які викладає НПП** | Теоретичні основи захисту інформації |
| **Напрями наукових досліджень** | Інформаційна безпека |
| **Посилання на реєстри ідентифікаторів для науковців** | ORCID: https://orcid.org/0000-0003-2608-6781<br>Google Scholar: https://scholar.google.com.ua/citations?user=WBfH9f4AAAAJ |
| Контактна інформація викладача: | |
| **E-mail:** | |
| **Контактний тел.** | +380507417375 |
| **Телефон кафедри** | |
| **Портфоліо викладача на сайті кафедри/Інституту/Академії** | |

**Анотація курсу.** Курс «Теоретичні основи захисту інформації» спрямований на формування у здобувачів вищої освіти системного уявлення про сутність, завдання та принципи інформаційної безпеки, її місце в системі державного управління, корпоративної політики та господарської діяльності. У межах дисципліни розглядаються організаційно-правові та методологічні засади створення і розвитку системи інформаційної безпеки підприємств та установ, класифікація кіберзагроз і ризиків, механізми управління інформаційними ресурсами, а також взаємозв'язок інформаційної безпеки з економічною, кадровою та організаційною безпекою. Особлива увага приділяється захисту конфіденційних даних, безпеці інформаційних систем і мереж, забезпеченню безперервності діяльності організацій, а також сучасним викликам у сфері кіберзлочинності, шкідливого програмного забезпечення, соціальної інженерії та кризових ситуацій, пов'язаних з інформаційними загрозами.

**Предмет вивчення дисципліни** є закономірності організації, функціонування та розвитку системи Теоретичні основи захисту інформації, її інституційно-правове та управлінське забезпечення, механізми взаємодії між державними інституціями, бізнес-структурами та громадянським суспільством, а також методи ідентифікації, попередження, нейтралізації й мінімізації кіберзагроз. У центрі уваги перебувають правові гарантії захисту інформації, система моніторингу та контролю ризиків, а також використання отриманої інформації для стратегічного планування та антикризового управління.

**Метою курсу** «Теоретичні основи захисту інформації» є формування у здобувачів вищої освіти базових знань про сутність, принципи, функції та напрями інформаційної безпеки, розвиток умінь аналізувати її правове регулювання та практику застосування, а також набуття навичок оцінювання ефективності заходів у сфері управління інформаційними ризиками, захисту даних і забезпечення стабільного функціонування організацій.

**Завдання навчальної дисципліни** «Теоретичні основи захисту інформації» полягають у тому, щоб ознайомити студентів із правовою базою та міжнародними стандартами інформаційної та кібербезпеки, сформувати розуміння її ролі у забезпеченні стабільності діяльності підприємств та установ, виробити вміння аналізувати співвідношення правових, організаційних та управлінських механізмів захисту інформації, оцінювати ризики та загрози, що виникають у внутрішньому й зовнішньому середовищі, а також розвинути здатність застосовувати отримані знання у практичній діяльності. Курс покликаний підготувати ґрунт для засвоєння спеціалізованих дисциплін, що деталізують окремі напрями захисту інформації, кібербезпеки та управління ризиками.

**Пререквізити навчальної дисципліни.** Вивчення навчальної дисципліни «Теоретичні основи захисту інформації не пов'язане з іншими дисциплінами.

**Постреквізити навчальної дисципліни.** Знання та уміння, отримані студентами в процесі вивчення навчальної дисципліни «Теоретичні основи захисту інформації», сприяють успішному вивченню здобувачами вищої освіти цілої низки інших навчальних дисциплін, спрямованих на формування професійних знань і умінь.

**Програмні компетентності**

| | |
|---|---|
| **Інтегральна компетентність (ІК)** | Здатність розв'язувати складні спеціалізовані та професійні завдання та вирішувати практичні проблеми в галузі національної безпеки, що передбачає здійснення кваліфікованого аналізу, пояснення та прогнозування безпекових явищ і характеризується комплексністю та невизначеністю умов. |
| **Загальні компетентності (ЗК)** | ЗК2. 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, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.<br>ЗК4. Знання основних методів наукового пошуку; вміння узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати наукової діяльності, здатність використовувати статистичні методи в професійній діяльності.<br>ЗК4. Знання основних методів наукового пошуку; вміння узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати наукової діяльності, здатність використовувати статистичні методи в професійній діяльності.<br>ЗК8. Здатність використовувати інформаційні та комунікаційні технології. |
| **Спеціальні (фахові) компетентності (СК)** | СК7. Здатність визначати основні властивості об'єктів безпеки в окремих сферах забезпечення національної безпеки і видах діяльності.<br>СК8. Здатність визначати основні положення щодо методів та заходів забезпечення безпеки держави у різноманітних сферах життєдіяльності. |
| **Програмні результати навчаня (ПРН)** | ПРН3. Застосовувати результати абстрактного мислення, самостійного пошуку, аналізу та синтезу, методів теорії інформації, теорії систем та системного аналізу для ефективного вирішення завдань професійної діяльності.<br>ПРН4. Використовувати знання з основних методів наукового пошуку; вміння узагальнювати отримані результати, обробки та аналізу інформації з різних джерел, оформлення та презентування результатів наукової діяльності, здатності використовувати статистичні методи в професійній діяльності.<br>ПРН5. Застосовувати знання державної та іноземних мов, інформаційно- комунікаційних технологій, комп'ютерної техніки для забезпечення професійної комунікації. |

**Зміст навчальної дисципліни**

| № | Назва теми | К-сть годин, з них: | | | |
|---|---|---|---|---|---|
| | | **Лекції** | **Семінарські зан.** | **Самостійна робота** | **Методи навчання/методи оцінювання** |
| **1 семестр**<br>**Модуль 1. Теоретико-методологічні засади управління інформаційною безпекою** | | | | | **Методи навчання:** словесні (навчальна лекція; бесіда; навчальна дискусія); індуктивний метод; дедуктивний метод; традуктивний метод; аналітичний; синтетичний; практичний (робота з фабулами юридичних справ); пояснювально-ілюстративний; репродуктивний; метод |
| Тема 1. | Поняття, сутність та завдання інформаційної безпеки. | 1 | 2 | 5 | |
| Тема 2. | Основні принципи та функції Теоретичні основи захисту інформації. | 1 | 2 | 5 | |
| Тема 3. | Класифікація інформаційних загроз і ризиків у діяльності організацій. | 1 | 2 | 5 | |

| | | | | |
|---|---|---|---|---|
| Тема 4. | Теоретичні підходи до формування системи Теоретичні основи захисту інформації. | 1 | 2 | 5 |
| Тема 5. | Взаємозв'язок інформаційної безпеки з економічною, організаційною та національною безпекою. | 1 | 2 | 5 |
| **Модуль 2. Нормативно-правові та інституційні основи інформаційної безпеки** | | | | |
| Тема 6. | Законодавча та нормативна база України у сфері інформаційної безпеки. | 1 | 2 | 5 |
| Тема 7. | Міжнародні стандарти і стратегії у сфері інформаційної та кібербезпеки (ISO/IEC 27001, NIS2, DORA). | 1 | 2 | 5 |
| Тема 8. | Інституційне забезпечення інформаційної безпеки: роль державних структур та корпоративних органів управління. | 1 | 2 | 5 |
| Тема 9. | Політика інформаційної безпеки організацій: структура, завдання, контроль. | 1 | 2 | 5 |
| Тема 10. | Механізми корпоративної відповідальності та етичні стандарти у сфері інформаційної безпеки. | 1 | 2 | 5 |
| **Модуль 3. Організаційно-управлінські механізми захисту інформації** | | | | |
| Тема 11. | Управління інформаційними ризиками та інцидентами. | 2 | 2 | 6 |
| Тема 12. | Система технічного захисту інформації та кіберзахисту. | 2 | 2 | 6 |
| Тема 13. | Організація контролю доступу та управління ідентифікацією користувачів. | 2 | 2 | 6 |
| Тема 14. | Інформаційна безпека персоналу: кадрова політика та внутрішні загрози. | 2 | 2 | 6 |
| Тема 15. | Репутаційна безпека, захист корпоративних даних та реагування на кризові інформаційні ситуації. | 2 | 2 | 6 |
| **Модуль 4. Сучасні виклики та перспективи Теоретичні основи захисту інформації** | | | | |
| Тема 16. | Протидія кіберзлочинності та соціальній інженерії. | 2 | 2 | 6 |

проблемного викладу; частково-пошуковий; дослідницький; інтерактивні методи (аналіз ситуацій; дискусії, дебати, полеміки; діалог, синтез думок; мозковий штурм; відпрацювання навичок; ситуативне моделювання, опрацювання дискусійних питань); моделювання професійної діяльності; інноваційні методи навчання (компетентнісний; проєктно-дослідницький); кейс-метод.

**Методи оцінювання:** усний контроль (усне опитування, оцінювання участі у дискусіях, інших інтерактивних методах навчання); письмовий контроль (контрольні, самостійні роботи, реферати); тестовий контроль (тести закритої форми: тест-альтернатива, тест-відповідність); метод самоконтролю та самооцінки; оцінювання кейс-завдань.

| | | | | | |
|---|---|---|---|---|---|
| Тема 17. | Корупційні ризики та внутрішні загрози в інформаційних системах організацій. | 2 | 2 | 6 | |
| Тема 18. | Кризове управління та стратегічне планування інформаційної безпеки. | 2 | 2 | 6 | |
| Тема 19. | Використання новітніх технологій (штучний інтелект, блокчейн, Big Data) у сфері інформаційної безпеки. | 2 | 2 | 6 | |
| Тема 20. | Перспективи розвитку Теоретичні основи захисту інформації в умовах цифрової трансформації та гібридних загроз. | 2 | 2 | 6 | |
| | | | | | |
| Модульна контрольна робота | | | | | |
| **Всього:** | | **30** | **40** | **110** | |
| **Форма контролю: екзамен** | | | | | |

Зміст самостійної роботи здобувача освіти з навчальної дисципліни «Теоретичні основи захисту інформації» передбачає підготовку до аудиторних занять шляхом опанування матеріалів лекції, вивчення базової і додаткової літератури, періодичних видань, Інтернет-джерел та судової практики, виконання практичних завдань (написання рефератів, аналіз проблемних ситуацій, підготовка результатів власних досліджень до виступу на конференціях, участь в конкурсах наукових робіт, підготовці та публікації наукових статей, тез тощо) протягом семестру; самостійне опрацювання окремих тем навчальної дисципліни; підготовку доповідей та презентацій за тематикою практичних занять; переклад іноземних текстів установлених обсягів; виконання індивідуальних завдань; підготовку до усіх видів контролю, у тому числі модульних контрольних робіт і підсумкової атестації; підготовку юридичних документів, інші види діяльності, що використовуються в Академії, Інституті і кафедрі.

Зміст самостійної роботи здобувача освіти визначається робочою програмою навчальної дисципліни конкретної навчальної дисципліни, методичними рекомендаціями для завданнями та рекомендаціями викладача.

Технічне обладнання та/або програмне забезпечення. В освітньому процесі використовуються навчальні аудиторії, бібліотека, мультимедійний проектор та комп'ютер для проведення лекційних та семінарських занять з елементам презентації. Вивчення окремих тем і виконання практичних завдань потребує доступу до інформації зі всесвітньої мережі Інтернет, який забезпечується безкоштовною мережею Wi-Fi.

**Форми методи контролю.**

Контроль успішності здобувачів освіти поділяється на поточний і підсумковий (семестровий).

Поточний контроль здійснюють під час проведення практичних, лабораторних і семінарських занять, метою якого є систематична перевірка розуміння та засвоєння теоретичного навчального матеріалу, уміння використовувати теоретичні знання під час виконання практичних завдань тощо. Можливості поточного контролю є надзвичайно

широкими: мотивація навчання, стимулювання навчально-пізнавальної діяльності, диференційований підхід до навчання, індивідуалізація навчання тощо.

Форми участі студентів у навчальному процесі, які підлягають поточному контролю:

-виступ з основного питання;

-усна доповідь;

- доповнення, запитання до того, хто відповідає;

- систематичність роботи на семінарських заняттях, активність під час обговорення питань;

- участь у дискусіях, інтерактивних формах організації заняття;

- аналіз законодавства та монографічної літератури;

- письмові завдання (тестові, контрольні, творчі роботи, реферати тощо);

- підготовка тез, конспектів навчальних або наукових текстів;

- самостійне опрацювання тем;

Контроль успішності здобувачів освіти поділяється на поточний і підсумковий .

Методи поточного контролю: усний контроль (опитування, бесіда, доповідь, повідомлення тощо); письмовий контроль (контрольна робота, реферат, виклад матеріалу на задану тему в письмовій формі тощо); комбінований контроль; презентація самостійної роботи; спостереження як метод контролю; тестовий контроль; проблемні ситуації.

**Система оцінювання та вимоги.**

**Таблиця розподілу балів, які отримують здобувачі вищої освіти***

**1-й семестр**

| | Поточний контроль знань | | | | | | | | | | Модульна контрольна робота | Залік** | Загальна кількість балів |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Теми | Тема 1 | Тема 2 | Тема 3 | Тема 4 | Тема 5 | Тема 6 | Тема 7 | Тема 8 | Тема 9 | Тема 10 | 20 | 20** | 100 |
| Робота на семінарському занятті | 10 | | 10 | | 5 | 10 | | 5 | 10 | | | | |
| Самостійна робота | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | | | |

*Таблиця містити інформацію про максимальні бали за кожен вид навчальної роботи здобувача вищої освіти.

Під час оцінювання засвоєння кожної теми за поточну навчальну діяльність здобувачу освіти виставляють оцінки з урахуванням затверджених критеріїв оцінювання для відповідної дисципліни.

Критерії оцінювання результатів навчання здобувачів освіти та розподіл балів, які вони отримують, регламентуються Положенням про оцінювання навчальних досягнень здобувачів вищої освіти у ПрАТ «ВНЗ «МАУП».

Модульний контроль. Модульна контрольна робота з навчальної дисципліни «Актуальні проблеми конституційного права України» проводиться на останньому занятті модуля у

письмовій формі, у вигляді тестування, а саме, тести закритої форми: тест-альтернатива, тест-відповідність на основі аналізу фабул юридичних справ.

Критерії оцінювання модульної контрольної роботи з навчальної дисципліни «Актуальні проблеми конституційного права України»:

при оцінюванні модульної контрольної роботи враховується обсяг і правильність виконаних завдань:

- оцінка «відмінно» (A) ставиться за правильне виконання всіх завдань (або більше 90% усіх завдань);

- оцінка «добре» (B) ставиться за виконання 80% усіх завдань;

- оцінка «добре» (C) ставиться за виконання 70% усіх завдань;

- оцінка «задовільно» (D) ставиться, якщо правильно виконано 60% запропонованих завдань;

- оцінка «задовільно» (E) ставиться, якщо правильно виконано більше 50% запропонованих завдань;

- оцінка «незадовільно» (FX) ставиться, якщо завдань виконано менше від 50 %.

Неявка на модульну контрольну роботу – 0 балів.

Вище наведені оцінки трансформуються в рейтингові бали у такий спосіб:

«A» – 18-20 балів;

«B» – 16-17 балів;

«C» – 14-15 балів;

«D» – 12-13 балів.

«E» – 10-11 балів;

«FX» – менше 10 балів.

Підсумковий семестровий контроль з навчальної дисципліни «Теоретичні основи захисту інформації є обов'язковою формою оцінювання результатів навчання здобувача вищої освіти. Він проводиться в терміни, встановлені графіком навчального процесу, та в обсязі навчального матеріалу, визначеного програмою навчальної дисципліни.

Підсумковий контроль проводиться у формі **заліку** (письмово). Студента допускають до семестрового контролю за умови виконання ним усіх видів робіт.

Семестровий контроль у формі заліку передбачає, що підсумкова оцінка з дисципліни визначається як сума (проста або зважена) балів за змістовими модулями. Залік виставляється за результатами роботи здобувача освіти впродовж усього семестру. Рейтингова оцінка здобувача освіти складається з балів, отриманих здобувачем за результатами заходів поточного контролю, заохочувальних балів.

Здобувачі освіти, які виконали всі умови допуску до заліку та мають рейтингову оцінку 60 і більше балів, отримують відповідну до набраного рейтингу оцінку без додаткових випробувань.

******Зі здобувачами, які виконали всі умови допуску до заліку та мають рейтингову оцінку менше 60 балів, а також з тими здобувачами, хто бажає підвищити свою рейтингову оцінку, на останньому за розкладом занятті з дисципліни в семестрі викладач проводить підсумковий семестровий контроль у вигляді заліку.

**Оцінювання додаткових (індивідуальних) видів навчальної діяльності.** До додаткових (індивідуальних) видів навчальної діяльності відносять участь здобувачів у роботі наукових конференцій, наукових гуртків здобувачів і проблемних груп, підготовці публікацій,

участь у Всеукраїнських олімпіадах і конкурсах та Міжнародних конкурсах тощо понад обсяги завдань, які встановлені відповідною робочою програмою навчальної дисципліни.

За рішенням кафедри здобувачам освіти, які брали участь у науково-дослідній роботі та виконували певні види додаткових (індивідуальних) видів навчальної діяльності, можуть присуджуватися заохочувальні (бонусні) бали за визначену освітню компоненту.

Також, заохочувальні бали можуть нараховуватися, якщо здобувач освіти, наприклад, виконав і захистив певні види робіт, відвідував всі лекції, семінарські й практичні заняття, має власний рукописний конспект лекцій та опрацьований додатковий навчальний матеріал, немає пропусків занять без поважних причин, відвідував додаткові консультації за участі лектора тощо.

Сума заохочувальних балів враховується при виставленні підсумкових балів в заліково-екзаменаційну відомість (але не більше **89 балів** в загальному підсумку) і може бути автоматично зарахована при виставленні підсумкової семестрової оцінки з відповідної освітньої компоненти.

Заохочувальні бали не є нормативними і не входять до таблиці розподілу балів, які отримують здобувачі вищої освіти та основної шкали системи оцінювання.

Один захід може бути підставою для виставлення заохочувальних балів лише за однією найбільш релевантною освітньою компонентою.

Підсумкова кількість балів, набрана здобувачами освіти за виконання завдань з самостійної роботи, є однією з складових поточної успішності з навчальної дисципліни. Самостійна робота з кожної теми за робочою програмою навчальної дисципліни оцінюється в діапазоні від 0 до 3 балів з використанням стандартизованих узагальнених критеріїв оцінювання знань.

**Шкала оцінювання виконання самостійної роботи (індивідуальних завдань)**

| Можлива максимальна оцінка виконання самостійної роботи (індивідуальних завдань) | Рівень виконання | | | |
|---|---|---|---|---|
| | Відмінний | Добрий | Задовільний | Незадовільний |
| 3 | 3 | 2 | 1 | 0 |

Для оцінювання результатів навчання здобувача вищої освіти впродовж семестру застосовується 100-бальна, національна та шкала ЄКТС оцінювання

**Шкала підсумкового оцінювання: національна та ECTS**

| Сума балів за всі види навчальної діяльності | Оцінка ECT8 | Оцінка за національною шкалою | |
|---|---|---|---|
| | | для екзамену, курсового проекту (роботи), практики | для заліку |
| 90 – 100 | A | відмінно | Зараховано |
| 82-89 | B | добре | |
| 75-81 | C | | |
| 68-74 | D | задовільно | |
| 60-67 | E | | |
| 35-59 | FX | незадовільно з можливістю повторного складання | не зараховано з можливістю повторного |
| 0-34 | F | незадовільно з обов'язковим повторним вивченням дисципліни | не зараховано з обов'язковим повторним вивченням дисципліни |

**Політика курсу.**

Для успішного засвоєння курсу «Теоретичні основи захисту інформації» здобувач освіти має:

- регулярно відвідувати лекційні та практичні заняття;
- систематично, системно й активно працювати на лекційних і практичних заняттях;
- відпрацьовувати пропущені заняття або незадовільні оцінки, отримані на заняттях;
- виконувати у повному обсязі завдання, які вимагає підготувати викладач, належна їх якість;
- виконувати контрольні та інші самостійні роботи;
- дотримуватися норм академічної поведінки та етики.

Курс «Теоретичні основи захисту інформації» передбачає засвоєння та дотримання принципів етики та академічної доброчесності, зокрема орієнтації на запобігання плагіату у будь-яких його проявах: всі роботи, доповіді, есе, реферати та презентації мають бути оригінальними та авторськими, не переобтяженими цитатами, що мають супроводжуватися посиланнями на першоджерела. Порушеннями академічної доброчесності вважаються: академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво, необ'єктивне оцінювання.

Оцінювання здобувача освіти орієнтовано на отримання балів за активність на семінарських заняттях, виконання завдань для самостійної роботи, а також виконання завдань, які здатні розвинути практичні уміння та навички за які можуть бути, за рішенням викладача, нараховані додаткові (бонусні) бали (участь у круглих столах, наукових конференціях, олімпіадах та наукових конкурсах серед студентів).

## Рекомендовані джерела

### Основна література

1. Смірнов О. А., Віхрова Л. Г., Осадчий С. І., Ковтун В. Ю., Мелешко Є. В. Основи захисту інформації: навч. посібник. – Кіровоград: КНТУ, 2011. – 322 с. – URL: http://dspace.kntu.kr.ua/jspui/handle/122456789/9799 :contentReference[oaicite:1]{index=1}

2. Смірнов О. А., Стасєв Ю. В., Бараннік В. В. Захист інформації в автоматизованих системах управління: навч. посібник. – Харків: ХУПС, 2015. – 264 с. – URL: [PDF] :contentReference[oaicite:2]{index=2}

3. Смірнов О. А., Кавун С. В., Доренський О. П., Вялкова В. І. Інформаційна безпека в комп'ютерних мережах: навч. посібник. – Кіровоград: РВЛ КНТУ, 2016. – 151 с. – URL: [PDF] :contentReference[oaicite:3]{index=3}

4. Смірнов О. А., Гнатюк С. О., Кавун С. В., Терейковський І. А., Жмурко Т. О., Смірнов С. А., Коваленко А. С. Основи безпеки в комп'ютерних мережах: навч. посібник. – Кропивницький: вид. Лисенко В. Ф., 2018. – 177 с. – URL: [PDF] :contentReference[oaicite:4]{index=4}

5. Бабак В. П., Ключников О. О. Теоретичні основи захисту інформації: підручник. – Київ: ІСПНПП, 2017. – URL: https://www.ispnpp.kiev.ua/tozi/ :contentReference[oaicite:5]{index=5}

6. Рибальський О. В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації: посібник для курсантів ВНЗ МВС України. – Київ: НАВС, 2012. – 104 с. – URL: https://nni1.navs.edu.ua/files/KIT/posibnuk%20tzi.pdf :contentReference[oaicite:6]{index=6}

7. Лужецький В. А. Основи інформаційної безпеки: навч. посібник. – URL: https://www.duikt.edu.ua/uploads/l_445_69621561.pdf :contentReference[oaicite:7]{index=7}

8. Тарнавський Ю. А. Технології захисту інформації: підручник [Електронний ресурс]. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с. – URL: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf :contentReference[oaicite:8]{index=8}

9. Пономаренко В. С., Журавльова І. В. Основи захисту інформації: навч. посібник. – Харків: ХДЕУ, 2003. – 176 с. – URL: https://nubip.edu.ua/sites/default/files/u370/vk20-tehnologiyi_zahistu_informaciyi_kn_2023.pdf :contentReference[oaicite:9]{index=9}

10. Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Основи інформаційної безпеки: навч. посібник. – Вінниця: ВНТУ, 2018. – 316 с. – URL: https://pdf.lib.vntu.edu.ua/books/IRVC/Dudikevich_2018_316.pdf :contentReference[oaicite:10]{index=10}

11. Граєворовський Н., Новіков В. Безпека інформаційно-комунікаційних систем: розділ 4 «Теоретичні основи захисту інформації».

– URL: https://is.ipt.kpi.ua/pdf/Graivorovskyi_Novikov.pdf :contentReference[oaicite:11]{index=11}

12. Карачка А. Ф. Технології захисту інформації (лекції): підручний матеріал. – 2017. – URL: https://dspace.wunu.edu.ua/bitstream/316497/26564/1/lekzii.pdf :contentReference[oaicite:12]{index=12}

13. Семенов С. Г. Захист інформації в комп'ютерних системах: навч. посібник. – URL: https://www.dgma.donetsk.ua/docs/kafedry/avp/metod/_%D0%91%D0%9A%D0%9C%20%D0%9F%D0%BE%D1%81_%D0%B1%D0%BD%D0%B8%D0%BA.pdf :contentReference[oaicite:13]{index=13}

14. Стичинська А. Теоретичні основи політики інформаційної безпеки: наукова стаття. – 2021. – URL: https://grani.org.ua/index.php/journal/article/view/1661 :contentReference[oaicite:14]{index=14}

15. Основи інформаційної безпеки: навч. посібник (В.Б. Вишня, О.С. Гавриш, Е.В. Рижков). – Дніпро: ДДУВС, 2020. – 128 с. – URL: https://er.dduvs.edu.ua/bitstream/123456789/4206/1/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%B8%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8%20%D0%BD%D0%B0%D0%B2%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%2006.2019%20%283%29.pdf :contentReference[oaicite:15]{index=15}

16. Ostapov S. E., Євсеєв С. П., Король О. Г. Технологія захисту інформації: навч. посібник. – Харків: ХНЕУ, 2013. – 476 с. – URL: [PDF] :contentReference[oaicite:16]{index=16}

17. [Доповнення] ISO/IEC 27002:2013 – Code of practice for information security management. – URL: https://www.iso.org/standard/54533.html :contentReference[oaicite:17]{index=17} *(не ДСТУ, але корисно)*

18. [Доповнення] ISO/IEC 27000:2018 – Overview and vocabulary. – URL: https://www.iso.org/standard/75652.html :contentReference[oaicite:18]{index=18} *(не ДСТУ)*

19. [Доповнення] ISO/IEC 27001:2013 – Information security management systems – Requirements. – URL: https://www.iso.org/standard/54534.html :contentReference[oaicite:19]{index=19} *(не ДСТУ)*

20. Rashid A., Chivers H., Danezis G., Lupu E., Martin A. CyBOK: The Cyber Security Body of Knowledge. – 2019. – URL: – :contentReference[oaicite:20]{index=20} *(англ., для ширшого контексту)*