Прим. № __

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
ТА СТРАТЕГІЧНИХ КОМУНІКАЦІЙ
ЦЕНТР КІБЕРБЕЗПЕКИ
КАФЕДРА КІБЕРБЕЗПЕКИ

ПРОГРАМА
АТЕСТАЦІЙНОГО ІСПИТУ

галузь знань	25 Воєнні науки, національна безпека, безпека державного кордону
спеціальність	256 Національна безпека (за окремими сферами забезпечення і видами діяльності)
освітня професійна програма	Кіберзахист у сфері інформаційних технологій та кіберпросторі
рівень вищої освіти	другий (магістерський)
форма навчання	очна (денна) та заочна

КИЇВ – 2026

Програму розглянуто та схвалено на засіданні кафедри кібербезпеки від «10» жовтня 2025 р., протокол №9.

Завідувач кафедри кібербезпеки
ЦКБ ННІ ІБ СК НА СБ України
доктор технічних наук, професор

Анастасія ВАВІЛЕНКОВА

«10» 10 2025 р.

Програма обговорена та схвалена на засіданні вченої ради Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України, від «06» 11 2025 року, протокол № 3.

І. ПОЯСНЮВАЛЬНА ЗАПИСКА

1. Мета та завдання проведення екзамену:

1.1. Метою атестаційного іспиту з освітньо-професійної програми «Кіберзахит у сфері інформаційних технологій та кіберпросторі» є встановлення відповідності засвоєних здобувачами вищої освіти знань, умінь, навичок та інших компетентностей вимогам освітньої програми, а саме: формуванню та розвитку у здобувачів вищої освіти професійних компетентностей до розв'язування задач дослідницького та інноваційного характеру у галузі національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері) та організації і забезпечення кібербезпеки у сфері інформаційних технологій та кіберпросторі.

1.2. Основними завданнями проведення атестаційного іспиту з освітньо-професійної програми «Кіберзахит у сфері інформаційних технологій та кіберпросторі» є перевірка та контроль теоретичних знань і практичних навичок роботи щодо:

Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у галузі національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері), провадити діяльність, пов'язану із кіберзахистом у сфері інформаційних технологій та кіберпросторі.

- ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу.
- ЗК 2. Здатність приймати обґрунтовані рішення.
- ЗК 3. Здатність спілкуватися іноземною мовою.
- ЗК 4. Здатність проводити дослідження на відповідному рівні.
- ЗК 5. Усвідомлення рівних можливостей та гендерних проблем.
- ЗК 6. Здатність вчитися і оволодівати сучасними знаннями.

СК 1. Здатність здійснювати професійну діяльність у відповідних сферах національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері).

СК 2. Здатність аналізувати та оцінювати сучасний стан і тенденції розвитку міжнародних відносин та проблеми міжнародної безпеки, їх вплив на національну безпеку в контексті набуття Україною членства в НАТО.

СК 3. Здатність використовувати понятійно-категоріальний апарат теорії національної безпеки, аналізувати та розвивати структуру системи забезпечення національної безпеки та принципи її функціонування.

СК 4. Здатність аналізувати та прогнозувати розвиток безпекового середовища (глобальний, регіональний та національний аспекти) за окремими сферами забезпечення та видами діяльності (кіберзахист, забезпечення державної безпеки в інформаційній сфері).

СК 5. Здатність організовувати цілеспрямовану діяльність щодо формування і реалізації державної політики у сферах національної безпеки та оборони.

СК 6. Здатність організовувати заходи територіальної оборони, мобілізаційної підготовки та мобілізації у межах посадових обов'язків.

СК 7. Здатність інтегрувати знання та розв’язувати складні задачі національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері) у широких та/або мультидисциплінарних контекстах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності.

СК 8. Здатність використовувати відповідне програмне забезпечення (мови програмування, пакети) для реалізації загальних завдань протиборства в інформаційній сфері та спеціальних задач (операцій) у кіберпросторі.

СК 9. Здатність вирішувати складні завдання і проблеми побудови інформаційно-комунікаційних систем та забезпечення їх безпеки в інформаційній сфері та кіберпросторі.

1.3. Здобувачі вищої освіти повинні володіти наступними компетентностями (зазначається з урахуванням положень Національної рамки кваліфікацій, професійних стандартів, а також «Довідника користувача Європейської кредитно-трансферної системи (ЄКТС)»:

Результати навчання:

ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.

ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.

ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог.

ПРН 4. Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей.

ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.

ПРН 6. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації.

ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.

ПРН 8. Забезпечувати дотримання принципу гендерної рівності під час здійснення професійної діяльності.

ПРН 9. Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов’язаних з викликами глобальній, європейській та регіональній безпеці.

ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері).

ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності.

ПРН 12. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки.

ПРН 13. Організовувати та здійснювати керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності.

ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.

ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.

ПРН 16. Організовувати та спрямовувати діяльність фахівців з кіберзахисту у сфері інформаційних технологій та кіберпросторі; розробляти та впроваджувати заходи із кіберзахисту у сфері інформаційних технологій та кіберпросторі, самостійно та у взаємодії з контролюючими органами.

ПРН 17. Створювати та документально оформлювати організаційно-технічні та організаційно-правові моделі кіберзахисту, а також моделі захисту конфіденційності, організовувати та розробляти системи кіберзахисту у сфері інформаційних технологій та кіберпростору, здійснювати моніторинг та аудит інформаційної безпеки та кібербезпеки на підприємствах, установах та організаціях різних форм власності.

ПРН 18. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення

ПРН 20. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові

стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури

ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації

ПРН 23. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ПРН 24. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

ПРН 25. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

ПРН 26. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

ІІ. ПЕРЕЛІК ТЕМ ТА НАВЧАЛЬНИХ ЕЛЕМЕНТІВ, КОТРІ ВИНОСЯТЬСЯ НА АТЕСТАЦІЙНИЙ ІСПИТ З ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «КІБЕРЗАХИСТ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРПРОСТОРІ»

Тема 1. Аудит інформаційної безпеки та кібербезпеки

Роль та задачі сучасної системи аудиту, контролю та моніторингу якості кібернетичної безпеки. Кращі світові практики, стандарти і вимоги до проведення процедур аудиту кібернетичної безпеки. Аудит та моніторинг приватних/операційних процесів підприємства. Методи аналізу ризиків порушення сталих приватних/операційних процесів. Організація та послідовність дій реалізації процесу та етапів аудиту кібернетичної безпеки.

Тема 2. Організаційно-правове забезпечення кіберзахисту

Концептуальні засади інформаційної безпеки та кібербезпеки. Інтереси держави в інформаційній сфері. Загрози національній безпеці в інформаційній сфері та кіберсфері. Стратегії кібербезпеки провідних країн світу. Організаційно-правові засади забезпечення інформаційної безпеки та кібербезпеки України. Державна політика у сферах інформаційної безпеки та кібербезпеки України.

Тема 3. Методи і моделі протидії кіберзагрозам

Організація безпеки. Соціальна інженерія. Класифікація кіберзагроз. Стратегії здійснення кібератак. DoS та DDoS-атаки. Моделі кібератак. Логічний спосіб та спосіб надсилання великої кількості пакетів інформації на комп'ютер, що атакується. Приховування даних. Маскування даних. Стеганографія.

Алгоритми шифрування даних. Хеш-функції. Шифрування з симетричним та асиметричним ключем. Програмні засоби захисту даних в комп'ютерних мережах

Тема 4. Кіберзахист об'єктів критичної інфраструктури

Управління доступом користувачів до об'єктів критичної інфраструктури. Класифікація та характеристика моделей доступу користувачів до об'єктів критичної інфраструктури. Багатофакторна автентифікація користувачів та обладнання об'єкта критичної інфраструктури. Моніторинг мережевого трафіку інформації об'єкта критичної інформаційної інфраструктури.

Тема 5. Управління кіберінцидентами

Категоризація та життєвий цикл кіберінцидентів. Етапи процесу управління кіберінцидентами. Виявлення подій. Платформа MISP. Сортування та аналіз подій. Реагування та відновлення після кіберінциденту. Поліпшення можливостей в процесі управління подіями інформаційної безпеки. Моніторинг подій інформаційної безпеки. Центри операційної безпеки, їх основні функції, структура та ролі. Команди реагування на кіберінциденти SERT/CSIRT, їх відмінності. Засоби реагування на кіберінциденти. Рішення для захисту кінцевих точок EDR/XDR, SIEM/SOAR/xSOAR. Цифрові докази. Національне та міжнародне законодавство у сфері кібербезпеки.

III. ПОРЯДОК ПРОВЕДЕННЯ АТЕСТАЦІЙНОГО ІСПИТУ З ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «КІБЕРЗАХИСТ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРПРОСТОРІ»

Атестаційний іспит з освітньо-професійної програми «Кіберзахист у сфері інформаційних технологій та кіберпросторі» проводиться у формі усної співбесіди за екзаменаційними білетами. Іспит проводиться відповідно до затвердженого розкладу роботи за участю не менше половини її складу та при обов'язковій присутності керівника предметної підкомісії.

Перед початком іспиту проводиться інструктаж, на якому доводиться алгоритм проведення іспиту, критерії оцінювання та виявлення причин, що можуть вплинути на проведення атестації (стан здоров'я, відсутність, тощо).

Структура екзаменаційного білету: кожен білет містить чотири питання: два теоретичного характеру та два – практичного. За необхідності можуть ставитися додаткові питання.

Для підготовки відповіді студент готує письмові тези на окремих аркушах паперу, зареєстрованих у встановленому порядку. На підготовку відповідей з питань білета здобувачу освіти надається 30 хвилин, тривалість відповідь – до 15 хв.

Під час підготовки до відповіді забороняється користуватися підручниками, навчальними посібниками, нормативно-правовими актами та іншими допоміжними джерелами інформації. Студент, який не дотримується зазначених вимог або порушує встановлені правила на іспиті, відсторонюється від подальшого його складання.

У разі проведення іспиту дистанційно – обов'язково проводиться консультація зі здобувачами вищої освіти в режимі онлайн, під час якої доводиться алгоритм проведення іспиту, критерії оцінювання, спосіб зв'язку та інформаційні засоби та середовища, які будуть застосовані. Студенти повинні забезпечити робоче місце для виконання екзаменаційного завдання, що має безперебійний доступ до мережі Інтернет, та самостійність виконання завдання (100 % - автентичність); недотримання зазначених умов є підставою невизнання результатів екзамену.

Результати складання атестаційного іспиту з освітньо-професійної програми оголошуються здобувачам вищої освіти у день проведення заходу, після затвердження протоколів керівниками предметних комісій.

IV. КРИТЕРІЇ ОЦІНЮВАННЯ РІВНЯ СФОРМОВАНОСТІ ЗНАНЬ ТА ВМІНЬ. АЛГОРИТМ ОЦІНЮВАННЯ

Оцінювання рівня сформованості знань та умінь здобувачів вищої освіти відбувається відповідно до компетентностей, які визначені в Стандарті вищої освіти України зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності), затвердженого наказом Міністерства освіти і науки України від 23.12.2021 року № 1423 «Про затвердження стандарту вищої освіти зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для другого (магістерського) рівня вищої світи» та проводиться за 100-бальною шкалою.

Оцінку результатів виконання студентами кожного контрольного завдання ККР проводиться за багатобальною шкалою.

У зв'язку з тим, що рівень складності питань білету приблизно рівний, то максимальну кількість балів за кожне окреме питання доцільно встановити однаковою, рівною 25 балам. При цьому оцінку результатів виконання кожного питання білету рекомендується проводити з використанням критеріїв, наведених у табл. 1.

Таблиця 1

Відповідність рейтингових оцінок за окремі питання білету у балах оцінкам за національною шкалою

Оцінка в балах	Оцінка за національною шкалою	Критерії оцінки
23-25	Відмінно	Відмінне виконання лише з незначною кількістю помилок
21-22	Добре	Виконання вище середнього рівня з кількома помилками
19-20		В загальному вірне виконання з певною кількістю суттєвих помилок
17-18	Задовільно	Непогане виконання, але зі значною кількістю недоліків
15-16		Виконання задовольняє мінімальним критеріям
менше 15	Незадовільно	Виконання не задовольняє мінімальним критеріям

Загальна схема нарахування балів за завдання білету та переведення балів за екзамен визначається шляхом підсумовування балів за виконання окремих завдань білету, після чого визначається оцінка згідно з табл. 2.

Таблиця 2

Схема нарахування балів та переведення шкал оцінювання

Оцінка за шкалою ЄКТС	Визначення рівнів оцінок	За національною (4-бальною) шкалою	За 100–бальною шкалою
A	Відмінно – відмінне виконання лише з незначною кількістю помилок	5 (відмінно)	90—100
B	Дуже добре – вище середнього рівня, але з кількома помилками	4 (добре)	84—89
C	Добре – загалом правильна робота, але з певною кількістю помилок		75—83
D	Задовільно – непогано, але зі значною кількістю недоліків	3 (задовільно)	65—74

E	Достатньо – виконання задовольняє мінімальні вимоги		60—64
FX	Незадовільно - потрібна додаткова робота	2 (незадовільно)	35—59
F	Незадовільно - потрібна значна додаткова робота		1—34

V. ІНФОРМАЦІЙНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

5.1. Навчально-методична документація: робоча програма та тези лекцій навчальної дисципліни «Аудит інформаційної безпеки та кібербезпеки», робоча програма та тези лекцій навчальної дисципліни «Організаційно-правове забезпечення кіберзахисту», робоча програма та тези лекцій навчальної дисципліни «Методи та моделі протидії кібератакам», робоча програма та тези лекцій навчальної дисципліни «Кіберзахист об'єктів критичної інфраструктури», робоча програма та тези лекцій навчальної дисципліни «Управління кіберінцидентами».

5.2. Нормативно-правові акти: закони України, міжнародні нормативно-правові акти, відомча нормативно-правова база

Закони України:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017р. №2163-VIII: станом на 01 жовтня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення 01.10.2025).
2. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006р. №3475-IV: станом на 01 жовтня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення 01.10.2025).
3. Про критичну інфраструктуру: Закон України від 16.11.2021р. №1882-IX: станом на 01 жовтня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 01.10.2025).
4. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994р. №80/94-ВР: станом на 01 жовтня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення 01.10.2025).
5. Про доступ до публічної інформації: Закон України від 13.01.2011р. №2939-VI: станом на 01 жовтня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення 01.10.2025).

6. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017р. №2155-VIII: станом на 30 серпня 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення 30.08.2024).
7. Про захист персональних даних: Закон України від 01.06.2010р. №2297-VI: станом на 30 серпня 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 30.08.2024).

Укази Президента України:

8. Про Стратегію забезпечення державної безпеки: Указ Президента України від 16.02.2022 №56/2022. URL: https://www.president.gov.ua/documents/562022-41377 (дата звернення 01.10.2025).
9. Про Доктрину інформаційної безпеки України: Указ Президента України від 25.02.2017 №47/2017. URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення 01.10.2025).
10. Про Стратегію кібербезпеки України: Указ Президента України від 26.08.2021 №447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення 01.10.2025).

Постанови Кабінету Міністрів України:

11. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019р. №518: станом на 01 жовтня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення 01.10.2025).
12. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 22.07.2022р. №821: станом на 01 жовтня 2025 р. URL: https://zakon.rada.gov.ua/ laws/show/821-2022-%D0%BF#Text (дата звернення 01.10.2025).
13. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього: Постанова Кабінету Міністрів України від 28.04.2023р. №415: станом на 01 жовтня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text (дата звернення 01.10.2025).
14. Про деякі питання об'єктів критичної інфраструктури: Постанова Каб. Міністрів України від 09.10.2020р. №1109: станом на 01 жовтня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (дата звернення 01.10.2025).
15. Про деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Каб. Міністрів України від 09.10.2020р. №943: станом на 01

жовтня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text (дата звернення 01.10.2025).
16. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Каб. Міністрів України від 29.12.2021р. №1426: станом на 01 жовтня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text (дата звернення 01.10.2025).
17. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах: Постанова Каб. Міністрів України від 29.03.2006р. №373: станом на 01 жовтня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text (дата звернення 01.10.2025).

Нормативні документи з технічного захисту інформації:

18. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
19. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.
20. НД ТЗІ 1.1-005-2007 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.
21. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.
22. НД ТЗІ 1.5-002-2012 Класифікатор засобів технічного захисту інформації.
23. НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.
24. НД ТЗІ 2.5-008-2002 Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу «2».
25. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
26. НД ТЗІ 2.6-001-2011 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.
27. НД ТЗІ 2.7-009-2009 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.
28. НД ТЗІ 3.1-001-2007 Захист інформації на об’єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Передпроектні роботи.

29. НД ТЗІ 3.3-001-2007 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.
30. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

5.3. Література основна і додаткова з навчальної дисципліни

Основна література

1. Бондаренко І. Д., Шестаков В. І., Коновалов О. Ю., Шершов Р. А., Задерей Д.Ю. Виявлення вразливостей об’єктів критичної інфраструктури в кіберпросторі: практ. посіб. Київ: НА СБУ, 2023. 154 с.
2. Вавіленкова А.І., Добришин Ю.Є., Шатирко О.Ф. Методи і засоби захисту від кіберзагроз: навч. посіб. Київ : НА СБУ, 2025. 160 с.
3. Методи та засоби технічного захисту інформації: Опорний конспект лекцій [Електронний ресурс]: навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: В.М. Луценко, Д.О. Прогонов. – Електронні текстові дані (1 файл: 1,80 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 289 с.
4. Організаційно-правові основи забезпечення кібербезпеки: підруч./ М.М. Присяжнюк, А.І. Марущак, Д.С. Мельник, В.В. Остроухов, М.В. Гуцалюк, О.П. Ткаченко; за заг. Ред. М.М. Присяжнюка. Київ: Видавництво Ліра-К, 2023. 320 с.
5. Євсеєв С.П., Остапов С.Е., Король О.Г. Кібербезпека: сучасні технології захисту: навч. посіб. для студ. вищ. навч. закл. Львів: “Новий Світ- 2000”, 2019. – 678 с.
6. Мамченко С.М. Комплексні системи захисту інформації: Навч. посіб. / С.М. Мамченко, В.Д. Козюра, В.Д. Бровко. – Київ: Нац. Акад. СБУ, 2020. – 372 с.
7. Андрєєв В.І., Хорошко В.О., Чередніченко В.С., Шелест М.Є., Основи інформаційної безпеки. Підручник. – К.: вид. ДУІКТ, 2009. –292 с.
8. Харченко В.С., Яковлев С.В., Горбачик О.С. та ін. Забезпечення функціональної безпеки критичних інформаційно-керуючих систем: монографія/ за ред. В.С.Харченка, С.В.Яковлева. Харків: Константа, 2019. – 272 с.
9. Когут Ю. Кібервійна та безпека об’єктів критичної інфраструктури: Консалтингова компанія Сідкон, 2021. – 332 с.
10. Вавіленкова А.І. Методи і моделі протидії кібератакам: навч. посібник / А.І. Вавіленкова. – Київ, 2023. – 142 с.
11. Вавіленкова А.І. Теоретичні засади та практика управління кіберінцидентами / А. І. Вавіленкова: монографія. – К.: Нац. акад. СБУ, 2025. – 146 с.
12. Основи кіберпростору, кібербезпеки та кіберзахисту: Навч. посібник / В. М. Богуш, В. В. Богуш, В. Д. Бровко [та ін.]. - К. : Ліра-К, 2021. – 554 с.

13. Міжнародне співробітництво у сфері запобігання та протидії транснаціональній злочинності [Текст] : монографія / І. М. Леган. – Чернігів : НУ «Чернігівська політехніка», 2021. – 328 с.

14. Кібербезпека «суспільства знань»: Монографія / О. Д. Довгань, А. В. Тарасюк, Т. Ю. Ткачук. - К.; Одеса : Фенікс, 2021. – 176 с.

15. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

Допоміжна література:

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

2. Жилін А.В. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О.А. Успенський; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

3. Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів – Київ: ДУТ ННІЗІ, 2020. – 167 с.

Інформаційні ресурси (інтернет-джерела)

1. Державна служба спеціального зв'язку та захисту інформації України (http://www.dsszzi.gov.ua/dstszi/control/uk/index)
2. Команда реагування на комп’ютерні надзвичайні події України «CERT-UA» (http://www.cert.gov.ua/)
3. Науково-освітній ПОРТАЛ інформаційних технологій та інформаційної безпеки (IT&ISS) (http://itiss.nau.edu.ua)
4. Портал «Центр інформаційної безпеки» (http://www.bezpeka.com/ua)
5. Інститут спеціального зв’язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут» (http://iszzi.kpi.ua/index.php/ua/)