МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАВАТВЕРДЖУЮ
Перший проректор Державного університету інформаційно - комунікаційних технологій

Олександр КОРЧЕНКО
«30» квітня 2024 р.

ПРОГРАМА ВСТУПНОГО ВИПРОБУВАННЯ ЗІ СПЕЦІАЛЬНОСТІ 125 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

для здобуття третього (освітньо-наукового) рівня вищої освіти

Київ – 2024

Розробники:

Завідувач кафедри — Галина ГАЙДУР
Професор кафедри — Андрій КОЖУХІВСЬКИЙ

Гарант:

Директор ННІЗІ — Віталій САВЧЕНКО

Завідувач кафедри ІКБ — Галина ГАЙДУР

Директор ННІЗІ — Віталій САВЧЕНКО

Завідувач відділу організації Проведення підготовки та атестації Аспірантів та докторантів Наукового центру — Юрій ПОКАНЄВИЧ

Директор Наукового центру — Олександр ДРОБИК

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Абітурієнт з освітнім ступенем (освітньо-кваліфікаційним рівнем) магістр (спеціаліст) повинен

знати:

методи забезпечення кібербезпеки інформаційних систем на об’єктах інформаційної діяльності;

технології забезпечення кібербезпеки інформаційних комп’ютерних мереж;

технології криптографічного захисту інформації;

методи протидії технічним каналам витоку інформації;

організаційні засади захисту інформації;

методи виявлення закладних пристроїв прихованого зняття інформації;

методи управління інформаційною безпекою;

політики інформаційної безпеки;

методи створення та управління підрозділом інформаційної безпеки.

вміти:

застосовувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення у сфері інформаційної та кібербезпеки;

розробляти та впроваджувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування в сфері інформаційної та кібербезпеки;

досліджувати, розробляти і супроводжувати методи та засоби інформаційної та кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури;

аналізувати, розробляти і супроводжувати систему управління інформаційною та кібербезпекою організації;

досліджувати та забезпечувати безперервність бізнес/операційних процесів з метою визначення вразливостей інформаційних систем у відповідності до політики інформаційної або кібербезпеки організації;

контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної або кібербезпеки організації;

досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам;

досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури;

аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій.

ПРОГРАМА ФАХОВОГО ВИПРОБУВАННЯ

Розділ 1.
Методи та технології кібербезпеки

1.1. Методи забезпечення кібербезпеки інформаційних систем на об’єктах інформаційної діяльності

Визначення ключових факторів забезпечення кібербезпеки на основі NIST Cybersecurity Framework. Види вразливостей інформаційних систем. Організаційні міри оцінки ризиків інформаційних систем. Методи виявлення загроз в інформаційній системі. Засоби управління кібербезпекою та управління подіями. Джерела отримання даних для аналізу подій в інформаційних системах. Методи виявлення інцидентів. Методи розслідування кіберінцидентів.

1.2. Технології забезпечення кібербезпеки інформаційних комп’ютерних мереж.

Види загроз та їх наслідки в інформаційних комп’ютерних мережах. Хмарні технології в забезпеченні кібербезпеки. Технології захисту периметра інформаційної мережі. Технології забезпечення безпеки web-ресурсів. Сучасні технології управління доступом до інформаційної мережі. Технології забезпечення безпеки кінцевих точок.

1.3. Технології криптографічного захисту інформації

Сучасні системи криптографічного захисту інформації. Типи криптоатак. Основні принципи побудови і аналізу криптографічних систем за їх призначенням. Основні класи і види криптопротоколів. Загальна класифікація атак на протоколи. Стандарти криптопротоколів в Інтернеті.

Розділ 2.
Методи та засоби технічного захисту інформації

2.1. Методи протидії технічним каналам витоку інформації

Технічні канали витоку інформації. Визначення технічного каналу витоку інформації. Види каналів витоку інформації. Причини виникнення технічних каналів витоку інформації. Канали витоку візуальної інформації. Методи протидії витоку візуальної інформації. Канали витоку мовної інформації. Методи протидії витоку мовної інформації. Матеріально-речові канали витоку інформації. Методи протидії витоку інформації матеріально-речовим каналом. Канали витоку інформації, що обробляється в технічних засобах. Методи протидії витоку інформації, що обробляється в технічних засобах.

2.2. Організаційні засади захисту інформації

Об’єкт інформаційної діяльності. Порядок категоріювання об'єктів інформаційної діяльності. Організація захисту інформації в автоматизованих системах. Організаційні та технічні аспекти розмежування доступу та контроль за доступом в інформаційній системі захищеного документообігу. Впровадження та експлуатація систем і засобів автоматизованої обробки інформації з обмеженим доступом. Комплекс технічного захисту інформації. Комплексні системи захисту інформації. Порядок проектування та впровадження комплексних систем захисту інформації.

2.3. Методи виявлення закладних пристроїв прихованого зняття інформації.

Класифікація закладних пристроїв прихованого зняття інформації. Закладні пристрої з передачею по радіоканалу. Закладні пристрої з передачею по провідним каналам. Демаскуючі ознаки закладних пристроїв. Класифікація засобів виявлення та локалізації закладних пристроїв. Обладнання для виявлення закладних пристроїв. Індикатори поля. Апаратура радіоконтролю. Порядок контролю телефонних ліній та кіл електроживлення. Засоби придушення сигналів закладних пристроїв. Апаратура нелінійної локації. Способи та методи контролю приміщень на відсутність закладних пристроїв.

Розділ 3.
Методи та технології управління інформаційною безпекою

3.1. Методи управління інформаційною безпекою

Класифікація методів управління. Метод наукового управління. Метод адміністративного управління. Метод людських відносин. Метод кількісного підходу в управлінні. Процесний підхід в управлінні. Переваги та недоліки процесного підходу. Використання процесного підходу в управлінні інформаційною безпекою. Системний підхід в управлінні. Переваги та недоліки системного підходу. Використання системного підходу в управлінні інформаційною безпекою. Ситуаційний підхід в управлінні. Переваги та недоліки ситуаційного підходу. Використання ситуаційного підходу в управлінні інформаційною безпекою. Використання комбінацій різних підходів в управлінні інформаційною безпекою.

3.2. Політики інформаційної безпеки

Поняття політики інформаційної безпеки. Цілі та задачі політики інформаційної безпеки. Верхній, середній та нижній рівні політики безпеки. Розробка політики інформаційної безпеки на різних рівнях управління. Ранжування користувачів інформаційних ресурсів. Сертифікація та навчання користувачів. Основні заходи забезпечення інформаційної безпеки щодо персоналу. Управління ризиками. Координація діяльності в області

інформаційної безпеки. Поповнення і розподіл ресурсів. Стратегічне планування. Контроль діяльності в області інформаційної безпеки.

3.3. Методи управління підрозділом інформаційної безпеки

Ключові позиції відповідальності за інформаційну безпеку (CISO, BISO). Структура підпорядкованості. Профіль компетентності. Сертифікація CISO, функції CISO. Визначення чисельності підрозділу інформаційної безпеки. Набір, відбір, післядипломна освіта, навчання персоналу підрозділу інформаційної безпеки. Фінансування підрозділу інформаційної безпеки. Положення про структурні підрозділи, посадові інструкції. Сутність і види аудиту інформаційної безпеки підприємства. Етапи процесу аудиту. Методи проведення аудиту. Підготовка звіту за результатами аудиту.

ПЕРЕЛІК ПИТАНЬ

Розділ 1

1. Ключові фактори забезпечення кібербезпеки на основі NIST Cybersecurity Framework.
2. Види уразливостей інформаційних систем.
3. Організаційні міри оцінки ризиків інформаційних систем.
4. Методи виявлення загроз в інформаційній системі.
5. Засоби управління кібербезпекою та управління подіями.
6. Джерела отримання даних для аналізу подій в інформаційних системах.
7. Методи виявлення інцидентів кібербезпеки.
8. Методи розслідування кіберінцидентів.
9. Види загроз та їх наслідки в інформаційних комп’ютерних мережах.
10. Хмарні технології в забезпеченні кібербезпеки.
11. Технології захисту периметра інформаційної мережі.
12. Технології забезпечення безпеки web-ресурсів.
13. Сучасні технології управління доступом до інформаційної мережі.
14. Технології забезпечення безпеки кінцевих точок.
15. Сучасні системи криптографічного захисту інформації.
16. Типи криптоатак.
17. Основні принципи побудови і аналізу криптографічних систем за їх призначенням.
18. Основні класи і види криптопротоколів.
19. Загальна класифікація атак на протоколи.
20. Стандарти криптопротоколів в Інтернеті.

Розділ 2

1. Технічні канали витоку інформації. Визначення технічного каналу витоку інформації. Види каналів витоку інформації.

2. Канали витоку візуальної інформації. Причини виникнення. Методи протидії.

3. Канали витоку мовної інформації. Причини виникнення. Методи протидії.

4. Матеріально-речові канали витоку інформації. Причини виникнення. Методи протидії.

5. Канали витоку інформації, що обробляється в технічних засобах. Причини виникнення. Методи протидії.

6. Об’єкт інформаційної діяльності. Порядок категоріювання об'єктів інформаційної діяльності.

7. Порядок організації захисту інформації в автоматизованих системах.

8. Організаційні та технічні аспекти розмежування доступу та контроль за доступом в інформаційній системі захищеного документообігу.

9. Характеристика обов'язкових етапів робіт під час впровадження та експлуатації систем і засобів автоматизованої обробки інформації з обмеженим доступом.

10. Комплекс технічного захисту інформації.

11. Комплексні системи захисту інформації. Порядок проектування та впровадження.

12. Класифікація закладних пристроїв прихованого зняття інформації.

13. Закладні пристрої з передачею по радіоканалу. Закладні пристрої з передачею по провідним каналам.

14. Демаскуючі ознаки закладних пристроїв.

15. Класифікація засобів виявлення та локалізації закладних пристроїв.

16. Обладнання для виявлення закладних пристроїв. Індикатори поля. Апаратура радіоконтролю.

17. Порядок контролю телефонних ліній та кіл електроживлення.

18. Засоби придушення сигналів закладних пристроїв.

19. Апаратура нелінійної локації. Будова та порядок застосування.

20. Способи та методи контролю приміщень на відсутність закладних пристроїв.

Розділ 3.

1. Класифікація методів управління. Метод наукового управління.

2. Метод адміністративного управління. Метод людських відносин. Метод кількісного підходу в управлінні.

3. Процесний підхід в управлінні. Переваги та недоліки процесного підходу. Використання процесного підходу в управлінні інформаційною безпекою.

4. Системний підхід в управлінні. Переваги та недоліки системного підходу. Використання системного підходу в управлінні інформаційною безпекою.

5. Ситуаційний підхід в управлінні. Переваги та недоліки ситуаційного підходу. Використання ситуаційного підходу в управлінні інформаційною безпекою.

6. Порядок використання комбінацій різних підходів в управлінні інформаційною безпекою.

7. Поняття політики інформаційної безпеки. Цілі та задачі політики інформаційної безпеки.

8. Верхній, середній та нижній рівні політики безпеки. Розробка політики інформаційної безпеки на різних рівнях управління.

9. Методи ранжування користувачів інформаційних ресурсів. Сертифікація та навчання користувачів.

10. Основні заходи забезпечення інформаційної безпеки щодо персоналу.

11. Управління ризиками. Координація діяльності в області інформаційної безпеки.

12. Стратегічне планування діяльності підрозділу інформаційної безпеки. Поповнення і розподіл ресурсів.

13. Контроль діяльності в області інформаційної безпеки.

14. Ключові позиції відповідальності за інформаційну безпеку (CISO, BISO).

15. Структура підпорядкованості. Профіль компетентності. Сертифікація CISO, функції CISO.

16. Визначення чисельності підрозділу інформаційної безпеки.

17. Набір, відбір, післядипломна освіта, навчання персоналу підрозділу інформаційної безпеки.

18. Порядок фінансування підрозділу інформаційної безпеки.

19. Порядок розробки Положення про структурні підрозділи підрозділу інформаційної безпеки, посадові інструкції працівників.

20. Сутність і види аудиту інформаційної безпеки підприємства. Етапи процесу аудиту. Методи проведення аудиту. Підготовка звіту за результатами аудиту.

КРИТЕРІЇ ОЦІНЮВАННЯ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Програму вступного випробування (іспиту) зі спеціальності складено на підставі програм рівня вищої освіти магістра зі спеціальності «125 – Кібербезпека та захист інформації» у Державному університеті інформаційно-комунікаційних технологій.

Фахове вступне випробування (іспит) зі спеціальності передбачає оцінювання підготовленості вступника до здобуття вищої освіти ступеня доктора філософії за спеціальністю «125 – Кібербезпека та захист інформації» на основі здобутих раніше компетентностей в обсязі стандарту вищої освіти магістра з відповідної спеціальності.

Вступне випробування зі спеціальності проводиться у письмовій формі. Згідно з діючою в університеті системою комплексної діагностики знань результати складання вступних випробувань оцінюються за рейтинговою 100-бальною шкалою, та двобальною, семибальною шкалою A, B, C, D, E (зараховано), FX, F (не зараховано). Підсумкові оцінки виставляються та вносяться до екзаменаційної відомості. Знання та вміння, продемонстровані вступниками до аспірантури на вступних випробуваннях зі спеціальності, оцінюватимуться за 100-бальною шкалою. Вступники, які наберуть менш як 60 балів, позбавлятимуться права участі в конкурсі. В екзаменаційній відомості в національній та європейській системах оцінювання знань і при переведенні оцінки в систему ECTS викладач керується співвідношеннями, поданими нижче у таблиці 1.

Таблиця 1

Відповідність підсумкових рейтингових оцінок
у балах оцінкам за національною шкалою та шкалою ECTS

Оцінка в балах	**Оцінка за національною шкалою**	**Оцінка за шкалою ECTS**	
		Оцінка	**Пояснення**
90-100	Відмінно	A	Відмінно
83 – 89	Добре	B	Дуже добре
75 – 82		C	Добре
65 – 74	Задовільно	D	Задовільно
60 – 64		E	Достатньо
40 – 59	Незадовільно	FX	Незадовільно
0 – 39		F	Незадовільно

Загальні критерії оцінювання знань:

“A” (90-100) – Вступник виявляє особисті творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування й нахили.

“B” (82-89) – Вступник вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв’язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна.

“C” (75-81) – Вступник вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок.

“D” (64-74) – Вступник відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих.

“E” (60-63) – Вступник володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.

“FX” (35-59) – Вступник володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.

“F” (1-34) – Вступник володіє матеріалом на рівні елементарного розпізнавання і відтворення окремих фактів, елементів, об’єктів.

При оцінюванні знань і вмінь вступника увага звертається передусім на:

уміння визначати найсуттєвіші проблемні питання, що потребують концептуального вирішення;

наявність нестандартних елементів аналізу та діагностики; різноманітність використаних способів зіставлення інформації;

здатність до комбінування та рекомбінування вихідної інформації; глибину опрацювання проблеми;

адекватність запропонованих заходів виявленим проблемам; наявність чітко визначеної позиції вступника;

аргументованість, переконливість обґрунтування запропонованих рішень;

уміння стисло, послідовно і чітко викласти сутність і результати своїх пропозицій;

наявність посилань на джерела, з яких запозичена будь-яка інформація та дотримання етики цитування;

логічність, конкретність і переконливість та повноту відповідей на запитання;

здатність аргументовано захищати свої технічні пропозиції;

вільне володіння технічною термінологією;

загальний рівень підготовки студента.

На вступному випробуванні оцінюванню підлягають:

- володіння ключовими теоретичними знаннями про об’єкт дисципліни;
- здатність творчо мислити та синтезувати знання;
- уміння використовувати знання для розв’язання практичних завдань;
- точність виконання розрахунків, тощо.

Порядок нарахування додаткових балів за навчальні/наукові досягнення для вступників до аспірантури подано у таблиці 2.

Таблиця 2

Порядок нарахування додаткових балів за навчальні/наукові досягнення вступників до аспірантури

Навчальні та наукові досягнення	Код	Кількість балів
Міжнародний сертифікат з іноземної мови, отриманий за останні два роки, що підтверджує рівні B2-C2	$ДБ_1$	B2 – 5 C1 – 10 C2 – 15
Диплом лауреата премії НАН України для молодих	$ДБ_6$	10

учених та студентів вищих навчальних закладів за обраною спеціальністю*		
Стаття у науковому виданні, включеному до Переліку наукових фахових видань України (за обраною спеціальністю)**	$ДБ_7$	15 (Кожна стаття)
Наукова стаття у виданні, яке входить до міжнародних наукометричних баз (Scopus, WebofScience, Copernikusta інші) за обраною спеціальністю**	$ДБ_8$	25 (Кожна стаття)
Одноосібна монографія або розділ у колективній монографії, яка рекомендована до друку вченою радою чи ВНЗ**	$ДБ_9$	10
Участь у науковій всеукраїнській конференції (за умови опублікування тез доповіді) за обраною спеціальністю**	$ДБ_{10}$	5 (Кожна стаття)
Участь у науковій міжнародній конференції (за умови опублікування тез доповіді) за обраною спеціальністю**	$ДБ_{11}$	10 (Кожна теза)
Патент або авторське свідоцтво про винахід***	$ДБ_{12}$	20
Рекомендація Вченої ради до аспірантури (за наявності)	$ДБ_{13}$	5
Диплом магістра/спеціаліста з відзнакою	$ДБ_{14}$	10

* диплом, отриманий під час навчання в магістратурі;

** за період не більше трьох років до моменту вступу (в сумі не більше як 60 балів за публікації та участь у конференціях);

*** за період не більше трьох років до моменту вступу.

ЛІТЕРАТУРА

1. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. - April 16, 2018. – 55p. [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
2. ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines/ ISO, IEC. - 2019. -76p.
3. Kutub Thakur Cybersecurity Fundamentals: A Real-World Perspective / Thakur Kutub, Pathan Al-Sakib Khan // CRC Press. – 2020. – 305p. ISBN 13:9780367476489
4. Leslie F. Sikos (Editor) AI in Cybersecurity. Springer. – 2018. – 215p.
5. Scott E. Enterprise Cybersecurity Study Guide/ Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, Abdul Aslam // Apress. 2018. – 737p. ISBN-13 (pbk): 978-1-4842-3257-6
6. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект / В.Л. Бурячок, В. Б.Толубко, С.В. Дорошенко: К.: ДУТ, 2015 - 298 с.

7. Гребенніков В. Комплексні системи захисту інформації. Проектування, впровадження, супровід / В. Гребенніков – «Видавничі рішення», 2018. – 249 с.
8. ДСТУ 33960-96. Захист інформації. Технічний захист інформації. Основні положення. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836
9. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836
10. Закон України «Про доступ до публічної інформації».
11. Закон України «Про електронні документи та електронний документообіг». https://zakon.rada.gov.ua/laws/ show /851-15
12. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
13. Закон України «Про інформацію» https://zakon.rada.gov.ua/laws/main/2657-12
14. Закон України «Про основні засади забезпечення кібербезпеки України». https://zakon.rada.gov.ua/laws/main/2163-19
15. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем: підручник. К. ДУІКТ, 2010. – 316 с.
16. Кукарін О.Б. Електронний документообіг та захист інформації. Навчальний посібник. За загальною редакцією д. держ. упр. професора Н.В. Грицяк – К. НАДУ, 2015. – С. 84.
17. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. К. ДУТ, 2020. – С. 326. [Режим доступу: http://www.dut.edu.ua/uploads/l_2162_16683938.pdf].
18. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. Навчальний посібник. К. ДУТ. 2020. – С. 126. [Режим доступу: http://www.dut.edu.ua/uploads/l_2031_50136601.pdf].
19. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації // К.: Міленіум, 2020. – 326 с.
20. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління // К.: ДУТ, 2022. – 307 с.
21. Лаптєв О.А., Кузавков В.В., Хорошко В.О. Системи пошуку засобів негласого знімання акустичної інформації // К.: Міленіум, 2023. 280 с.
22. Ластівка Г.І., Шпатар П.М. Технічний захист інформації в інформаційних та телекомунікаційних системах. Навчальний посібник. Чернівці. Чернівецький національний університет, 2018. – С. 252.

23. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі. http://www.dut.edu.ua/uploads/1_1023_75718671.pdf
24. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.
25. 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.
26. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (зі зміною №1). http://www.dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407
27. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу «2». http://www.dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106343
28. НД ТЗІ 2.7-011-12 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки методики виявлення закладних пристроїв. http://www.dstszi.gov.ua/dsszzi/doccatalog/document%3Fid=103253
29. НД ТЗІ 3.6-003-2016 Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації.
30. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС. http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46075
31. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074
32. НД ТЗІ Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випрмінювання. Класифікація та загальні технічні вимоги. Рекомендації. http://www.dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden=1&art_id=101924&cat_id=89734&ctime=1344501363205
33. Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфроструктури» від 19.06.2010 № 518.
34. Постанова Кабінету Міністрів України «Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних» від 04.02.1998 №121. https://zakon.rada.gov.ua/laws/main/121-98-%D0%BF

35. Постанова Кабінету Міністрів України «Про затвердження Порядку підключення до глобальних мереж передачі даних» від 12.04.2002 р. № 522.
36. Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373. https://zakon.rada.gov.ua/laws/main/373-2006-%D0%BF
37. Постанова Кабінету Міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736.
38. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.
39. Тим Рейнс Cybersecurity Threats, Malware Trends, and Strategies: Mitigate exploits, malware, phishing, and other social engineering attacks. Packt Publishing. – 2020.- 429p. ISBN 978-1-80020-601-4.
40. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ – ПЕМВН-95). http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101798&cat_id=89734&ctime=1344500065981
41. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих систем і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95). http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=120206&cat_id=89769&ctime=1421836194327
42. Указ Президента України «Про положення про технічний захист інформації в Україні» від 27.09.1999 № 1229.
43. Чарльз Дж. Брукс Cybersecurity Essentials / Чарльз Дж. Брукс, Крейг Р. Филип, Шорт Дональд// Paperback: Sybex.- 2018.- 767p.

ПОРЯДОК ПРОВЕДЕННЯ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Склад предметної комісії визначається додатковим наказом в.о. ректора Державного університету інформаційно-комунікаційних технологій «Про створення предметних комісій з приймання вступних іспитів до аспірантури». Робота комісії та порядок проведення вступного випробування регламентується Правилами прийому до аспірантури для здобуття наукового

ступеня доктора філософії у Державному університеті інформаційно-комунікаційних технологій на навчальний рік.

Програму обговорено та схвалено на засіданні кафедри Інформаційної та кібернетичної безпеки.

Протокол № 9 від «02» квітня 2024 р.

Гарант освітньої програми
Голова предметної комісії
Директор Навчально-наукового інституту захисту інформації

доктор технічних наук, професор Віталій САВЧЕНКО