

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ  
Навчально-науковий інститут інформаційно-діагностичних систем  
Кафедра безпеки інформаційних технологій

ЗАТВЕРДЖУЮ  
Голова фахової атестаційної комісії  
\_\_\_\_\_ Філоненко С.Ф.  
« \_\_\_\_ » \_\_\_\_\_ 2016р.



## Система менеджменту якості


### ПРОГРАМА

додаткового вступного випробування  
(фахового вступного випробування)  
за освітньою програмою підготовки фахівців  
освітнього ступеня «Спеціаліст»

за спеціальністю 125 Кібербезпека

спеціалізація 7.17010302 «Адміністративний менеджмент у сфері захисту інформації»

**СМЯ НАУ П 14.01.06-01-2016**


	Система менеджменту якості <b>ПРОГРАМА</b> фахового вступного випробування за освітньою програмою підготовки фахівців освітнього ступеня «Спеціаліст»	Шифр документа	СМЯ НАУ П 14.01.06-01-2016
		Стор. 2 із 11	

## ВСТУП

**Мета** фахового вступного випробування – визначення рівня знань за напрямками професійної діяльності та формування контингенту студентів, найбільш здібних до успішного опанування дисциплін відповідних освітніх програм. Вступник повинен продемонструвати фундаментальні, професійно-орієнтовні знання та уміння, здатність вирішувати типові професійні завдання, передбачені програмою вступу.

Фахове вступне випробування проходить у письмовій формі шляхом вирішення завдань.


Організація фахового вступного випробування здійснюється відповідно до Положення про приймальну комісію Національного авіаційного університету.

	Система менеджменту якості <b>ПРОГРАМА</b> фахового вступного випробування за освітньою програмою підготовки фахівців освітнього ступеня «Спеціаліст»	Шифр документа	СМЯ НАУ П 14.01.06-01-2016
		Стор. 3 із 11	

Перелік програмних питань  
з дисциплін, які виносяться на фахове вступне випробування  
за освітньою програмою підготовки фахівців  
освітнього ступеня «Спеціаліст»

Назва дисципліни «Комплексні системи захисту інформації»

1. Визначення головних понять пов'язаних з КСЗІ.
2. Система законодавства у сфері інформаційних відносин.
3. Історичні аспекти формування поняття систем захисту інформації.
4. Критерії оцінки інформаційної безпеки за національними стандартами.
5. Класи автоматизованих систем.
6. Профілі захисту інформації.
7. Визначення області та межі дії КСЗІ.
8. Місце і роль КСЗІ в управлінні діяльністю організацій.
9. Загальні принципи внутрішньої та зовнішньої політики держави у сфері інформаційних відносин.
10. Організаційні та інженерно-технічні заходи.
11. Об'єкти інформаційних відносин.
12. Суб'єкти інформаційних відносин, основні права й обов'язки учасників зазначених відносин.
13. Нормативно-правове забезпечення КСЗІ.
14. Технічні канали витоку, нав'язування, знищення та блокування інформації в інформаційно-телекомунікаційних системах (ІТС).
15. Методи та засоби інженерно-технічних заходів безпеки.
16. Структура КСЗІ.
17. Обґрунтування створення КСЗІ.
18. Етапи побудови КСЗІ.
19. Ресурси як основні об'єкти КСЗІ.
20. Методика впровадження КСЗІ.
21. Розробка організаційно-розпорядчої документації на КСЗІ.
22. Документація КСЗІ.
23. Оцінка рівня загроз та вразливостей.
24. Системний підхід в управлінні КСЗІ.
25. Вимоги до проведення випробувань КСЗІ.
26. Програма, тривалість і область діяльності випробувань КСЗІ.
27. Експертиза КСЗІ.
28. Атестація КСЗІ.
29. Сертифікація КСЗІ.
30. Супроводження КСЗІ.

	Система менеджменту якості <b>ПРОГРАМА</b> фахового вступного випробування за освітньою програмою підготовки фахівців освітнього ступеня «Спеціаліст»	Шифр документа	СМЯ НАУ П 14.01.06-01-2016
	Стор. 4 із 11		

### *Основна література*


1. Конституція України.
2. Концепція національної безпеки.
3. Закон України „Про національну програму інформатизації” Київ-2001.
4. закон України „Про інформацію” Київ-1992.
5. Закон України "Про державну таємницю" Київ-1999.
6. Закон України "Про науково-технічну інформацію" Київ-1995.
7. Закон України "Про оперативно-розшукову діяльність" Київ-1992.
8. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" Київ-2003.
9. Закон України "Про електронні документи та електронний документообіг" Київ-2003.
10. Закон України "Про електронний цифровий підпис" Київ-2003.
11. Кримінальний Кодекс України. Київ-2001.
12. Закони України „ Про банки і банківську діяльність”, „ Про національний банк України”, Про платіжні системи та переказ грошей в Україні”. Київ-2000.
13. Хорошко В.О. та ін. „Захист інформації” КМУГА-2000.
14. Н.Ворожко В.П., Корченко О.Г. „Захист інформації з обмеженим доступом” КМУГА-1999.

### *Додаткова література*

1. ДСТУ 3396.0-96 та ДСТУ 3396.1-96. Захист інформації. ТЗІ.
2. [www.rada.gov.ua](http://www.rada.gov.ua) – офіційний сайт Верховної Ради України.
3. [www.dstszi.gov.ua/dstszi](http://www.dstszi.gov.ua/dstszi) - офіційний сайт ДСТЗІ.

### Назва дисципліни "Криптографія та стеганографія"

1. Основні характеристики захисту інформації та криптографічні методи їх забезпечення.
2. Шифрування та кодування.
3. Криптографія та стеганографія.
4. Забезпечення цілісності інформації. Однонаправлені криптографічні функції.
5. Аутентифікація користувача. Цифровий підпис.
6. Забезпечення доступності інформації. Протоколи обміну ключами.
7. Криптостійкість шифрів та ключів.
8. Основні вимоги до криптографічних алгоритмів.
9. Шифрування методом Цезаря та його зламування.
10. Шифрування методом простої підстановки та його зламування.
11. Поліалфавітні шифри. Шифрування методом Віженера та його зламування.
12. Шифрування методом простої перестановки та його зламування.
13. Лінійні перетворення. Шифри збивання.
14. Одноразові блокноти. Формування випадкової послідовності.
15. Комбінація шифрів. Алгоритм шифрування DES.
16. Асиметрична криптографія (криптографія з відкритими ключами).
17. Прості та складені числа та їх властивості.
18. Взаємно прості числа. Алгоритм Евкліда знаходження найбільшого спільного дільника.
19. Рівняння Діофанта. Знаходження секретного ключа.
20. Лишки та їх властивості.

	Система менеджменту якості <b>ПРОГРАМА</b> фахового вступного випробування за освітньою програмою підготовки фахівців освітнього ступеня «Спеціаліст»	Шифр документа	СМЯ НАУ П 14.01.06-01-2016
		Стор. 5 із 11	

21. Шифрування методом Рівеста-Шаміра-Адлемана.
22. Багаторівнева система ключів. Метод шифрування ель-Гамалія.
23. Еліптичні криві. Додавання точок на еліптичних кривих.
24. Алгоритм формування ключів на еліптичних кривих.
25. Алгоритм формування цифрового підпису на еліптичних кривих.
26. Алгоритм перевірки цифрового підпису на еліптичних кривих.
27. Стеганографічний захист інформації. Прихована інформація. Контейнер.
28. Пропускна спроможність стеганографічного каналу.
29. Криптографічні алгоритми та протоколи.
30. Довірчі криптографічні протоколи. Протоколи з арбітражем та судівством.

### *Основна література*


1. Б. Шнайер Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Изд-во ТРИУМФ.2002. - 816 с.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. - М.: Гелиос АРВ, 2001. - 480 с.
3. Анохин М. И., Варновский Н. П., Сидельников В. М., Яценко В. В. Криптография в банковском деле. - М.:МГУ, 1997.
4. Чмора АЛ. Современная прикладная криптография. - М.:Гелиос АРВ, 2001.-256 с.
5. Аграновский А.В., Хади Р.А. Практическая криптография: алгоритмы и их программирование. - М.:СОЛОН-Пресс, 2002. - 256 с.
6. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. - М.:КУДИЦ-ОБРАЗ, 2003.-240 с.
7. В.Г. Грибунин, Н.Н. Оков, И.В. Туринцев Цифровая стеганография. - М.: СОЛОН-Пресс, 2002. -272 с.
8. В.К. Задірака, О.С. Олексюк Комп'ютерна криптологія:підручник. - Київ:2002. - 504 с.
9. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основы комп'ютерної стеганографії. Навчальний посібник. - Вінниця: ВДГУ, 2003. -143 с.
10. Домашев А.В. и др. Программирование алгоритмов защиты информации. Учебное пособие. - М.: "Нолидж", 2000. - 288 с.
11. В.Мельников Защита информации в компьютерных системах. М.: "Финансы и статистика", 1997. – 368 с.

### *Додаткова література*

1. Довідкова система операційної системи Windows 2000.
2. В.К. Задірака, О.С. Олексюк Комп'ютерна арифметика багаторозрядних чисел: Наукове видання. - Київ:2003. - 264 с.
3. Введение в криптографию / Под общ. ред. В.В. Яценко.- 2-е изд., испр. - М.:МЦНМО:"ЧеРо", 1999.-271 с.
4. В. Жельников Криптография от папируса до компьютера. - М.:АВР, 1996.-336 с.
5. Фаль О.М. Криптография: основні ідеї та застосування: Преапринт. - К.: ІВЦ "Видавництво "Політехніка"", 2003. - 28 с.
6. Саломаа А. Криптография с открытым ключом / Пер. с англ. - М.: Мир, 1996.-318 с.
7. Вербицький О.В. Вступ до криптології. - Льв.:ВНТЛ, 1998. - 247 с.

Назва дисциплін «Системи менеджменту інформаційної безпеки»

1. Історичні аспекти формування поняття системи менеджменту.

	Система менеджменту якості <b>ПРОГРАМА</b> фахового вступного випробування за освітньою програмою підготовки фахівців освітнього ступеня «Спеціаліст»	Шифр документа	СМЯ НАУ П 14.01.06-01-2016
		Стор. 6 із 11	

2. Визначення області та межі дії систем менеджменту інформаційної безпеки.
3. Структура систем менеджменту.
4. Місце і роль системи менеджменту інформаційної безпеки в управлінні діяльністю організацій.
5. Критерії оцінки інформаційної безпеки за національними стандартами.
6. Критерії оцінки інформаційної безпеки міжнародними стандартами.
7. Канадські критерії оцінки безпеки надійних комп'ютерних систем.
8. Міжнародний стандарт ISO / IEC 15408.
9. Федеральні критерії оцінки інформаційної безпеки.
10. Історія серії стандартів ISO/IEC 27000.
11. Історія стандарту ISO/IEC 27001.
12. Обґрунтування створення СМІБ.
13. Структура та вимоги стандарту ISO/IEC 27001.
14. Структура стандарту ISO/IEC 27002.
15. Система управління ризиками на вимогу стандарту ISO/IEC 27001:2005.
16. Додаток А стандарту ISO/IEC 27001:2005. Реалізація вимог стандарту.
17. Методики впровадження системи менеджменту інформаційної безпеки.
18. Принципи QECD.
19. Модель PDCA.
20. Додаток В стандарту ISO/IEC 27001:2005.
21. Додаток С стандарту ISO/IEC 27001:2005.
22. Технології оцінки інформаційних ризиків.
23. Технології аналізу інформаційних ризиків.
24. Інтеграція системи менеджменту інформаційної безпеки за вимогами ISO/IEC 27001:2005 та системи менеджменту якості за вимогами ISO 9001:2000.
25. Вимоги стандарту ISO 19011:2002 до проведення аудитів.
26. Аудит систем менеджменту інформаційної безпеки.
27. Види аудиту.
28. Етапи внутрішнього аудиту систем менеджменту інформаційної безпеки.
29. Проведення коригувальних та попереджувальних дій.
30. Вимоги до аудиторів..


#### ***Основна література***

1. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навчальний посібник. / МОН. – К.: Кондор, 2008. – 383 с.
2. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів / В.П. Бабак, О.Г. Корченко. – К.: НАУ, 2003. – 670с.
3. Захист інформації в мережах передачі даних / О.І. Юдін, О.Г. Корченко, Г.Ф. Конахович – К.: Вид-во ТОВ «НВП»Інтерсервіс», 2009. – 716 с.
4. Корченко О.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: «МК-Пресс», 2006. – 320с.

#### ***Додаткова література***

1. Риск-менеджмент. / В.Н. Вяткин, И.В. Вяткин, В.А. Гамза, Ю.Ю. Екатеринославский, Дж.Дж Хэмптон; И. Юргенс, ред. Учебник. - М.: Дашков и К, 2003. - 494 с.
2. Информационная безопасность и защита информации: Учебное пособие. – 2-е изд., стер. / В. П. Мельников, С. А. Клейменов, А. М. Петраков; Клейменов С. А., ред. – М.: Академия, 2007. – 332 с.



	Система менеджменту якості <b>ПРОГРАМА</b> фахового вступного випробування за освітньою програмою підготовки фахівців освітнього ступеня «Спеціаліст»	Шифр документа	СМЯ НАУ П 14.01.06-01-2016
		Стор. 8 із 11	

Міністерство освіти і науки України  
Національний авіаційний університет

Навчально-науковий інститут інформаційно-діагностичних систем

Кафедра Безпеки інформаційних технологій

Освітній ступінь Спеціаліст

Спеціальність 125 Кібербезпека

Спеціалізація (освітня програма) 8. 17010302 Адміністративний менеджмент у сфері захисту інформації

ЗАТВЕРДЖУЮ  
Голова фахової атестаційної комісії  
\_\_\_\_\_ Філоненко С.Ф.  
підпис

Фахове вступне випробування

Білет № 1

Завдання 1. Шифрування методом Цезаря та його зламування.

Завдання 2. Додаток А стандарту ISO/IEC 27001:2005. Реалізація вимог стандарту.


Завдання 3. Програма, тривалість і область діяльності випробувань КСЗІ.

Затверджено на засіданні кафедри безпеки інформаційних технологій

Протокол № 3 від «21» березня 2016 р.

Завідувач кафедри \_\_\_\_\_ Корченко О.Г.



	Система менеджменту якості <b>ПРОГРАМА</b> фахового вступного випробування за освітньою програмою підготовки фахівців освітнього ступеня «Спеціаліст»	Шифр документа	СМЯ НАУ П 14.01.06-01-2016
		Стор. 9 із 11	


Рейтингові оцінки за виконання окремих завдань фахових вступних випробувань

Вид навчальної роботи	Максимальна величина рейтингової оцінки (бали)
Виконання завдання № 1	30
Виконання завдання № 2	30
Виконання завдання № 3	40
Усього:	100

Значення рейтингових оцінок в балах за виконання завдань вступних випробувань та їх критерії\*

Оцінка в балах за виконання окремих завдань			Критерій оцінки
18–20	27–30	36–40	Відмінне виконання лише з незначною кількістю помилок
17	25–26	33–35	Виконання вище середнього рівня з кількома помилками
15–16	23–24	30–32	У загальному вірне виконання з певною кількістю суттєвих помилок
14	20–22	27–29	Непогане виконання, але зі значною кількістю недоліків
12–13	18–19	24–26	Виконання задовольняє мінімальним критеріям
менше 12	менше 18	менше 24	Виконання не задовольняє мінімальним критеріям
<b>Увага! Оцінки менше, ніж 12, 18 або 24 бали не враховується при визначення рейтингу</b>			

\* Значення оцінок у балах та їх критерії відповідають вимогам шкали ECTS

	Система менеджменту якості <b>ПРОГРАМА</b> фахового вступного випробування за освітньою програмою підготовки фахівців освітнього ступеня «Спеціаліст»	Шифр документа	СМЯ НАУ П 14.01.06-01-2016
		Стор. 10 із 11	

### Відповідність рейтингових оцінок

у балах оцінкам за національною шкалою та шкалою ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
<b>90-100</b>	<b>Відмінно</b>	<b>A</b>	<b>Відмінно</b> (відмінне виконання лише з незначною кількістю помилок)
<b>82 – 89</b>	<b>Добре</b>	<b>B</b>	<b>Дуже добре</b> (вище середнього рівня з кількома помилками)
<b>75 – 81</b>		<b>C</b>	<b>Добре</b> (в загальному вірне виконання з певною кількістю суттєвих помилко)
<b>67 – 74</b>	<b>Задовільно</b>	<b>D</b>	<b>Задовільно</b> (непогано, але зі значною кількістю недоліків)
<b>60 – 66</b>		<b>E</b>	<b>Достатньо</b> (виконання задовольняє мінімальним критеріям)
<b>35 – 59</b>	<b>Незадовільно</b>	<b>FX</b>	<b>Незадовільно</b>
<b>1 – 34</b>		<b>F</b>	<b>Незадовільно</b>