Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ О.О. Ілляшенко
(підпис) (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Управління інформаційною безпекою
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2023 рік

Розробник: Брежнєв Є.В. професор кафедри 503, д.т.н., проф.
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол №1 від « 27 » 08 2023 р.

Завідувач кафедри д.т.н., професор В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4.5</td><td rowspan="9">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека"
(код та найменування)

Освітня програма
Безпека інформаційних і комунікаційних систем
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Цикл загально-професійної підготовки</td></tr>
<tr><td>Кількість модулів – 2</td><td rowspan="2">Навчальний рік
2023/2024</td></tr>
<tr><td>Кількість змістових модулів – 4</td></tr>
<tr><td>Індивідуальне завдання: не передбачено</td><td rowspan="2">Семестр: 8-й</td></tr>
<tr><td>Загальна кількість годин – 64/135</td></tr>
<tr><td rowspan="5">Кількість тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи студента – 4</td><td>Лекції [1)]32 год.</td></tr>
<tr><td>Практичні, семінарські
32 год.</td></tr>
<tr><td>Лабораторні[1)]
год.</td></tr>
<tr><td>Самостійна робота
65 год.</td></tr>
<tr><td>Індивідуальні завдання: 6 год.</td></tr>
<tr><td></td><td>Вид контролю:
модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:

Для денної форми навчання – 64/71.

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: є отримання студентами необхідних знань та навиків для діяльності на основі застосування системи теоретичних знань і практичних навичок; формування комплексу засобів (правил, процедур, тощо) щодо управління інформаційною безпекою; застосування комплексного підходу з забезпечення інформаційної безпеки в різних сферах діяльності (критичні системи та додатки).

Завдання: знати структуру нормативних актів та стандартів в сфері управління інформаційної безпекою; систему термінів та понять; організовувати основні

процеси реалізації систем ІБ, а саме, планування, ризик-аналізу, вибору контрзаходів, тощо; вміти використовувати сучасні інформаційні технології при оцінювання ризиків критичної інфраструктури; визначати шляхи зниження ризиків, практично застосовувати методи забезпечення безпеки.

Мати уявлення: про методики розрахунку ризиків інформаційної безпеки на підприємствах.

Програмні компетентності. Дисципліна має допомогти сформувати у студентів такі компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

Програмні результати навчання. В результаті вивчення дисципліни студенти мають досягти такі програмні результати навчання:

ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

ПРН 14. вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН 21 Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

Міждисциплінарні зв'язки:

Пререквізити. Дисципліна базується на: «Системи технічного захисту інформації», «Безпека операційних систем».

Кореквізити. Дисципліна є базовою для: «Нормативно-правове забезпечення інформаційної безпеки», «Комплексні системи захисту інформації: проектування, впровадження, супровід», «Комплексні системи захисту інформації: проектування, впровадження, супровід (КП)», «Курс на вибір 3 Технології захисту інформації», «Дипломний робота (проект) бакалавра».

3. Програма навчальної дисципліни

Модуль 1

Змістовний модуль 1

ТЕМА 1. Вступ до навчальної дисципліни «Управління інформаційною безпекою»

Місце дисципліни в системі підготовки фахівця із організації інформаційної безпеки. Визначення головних понять пов'язаних з управлінням інформаційною безпекою. Історичні аспекти формування поняття управління інформаційною безпекою.

Предмет дисципліни, її цілі та задачі. Структура, завдання і форми контролю, основна література. Основні положення. Визначення області та межі дії систем управління інформаційною безпекою.

ТЕМА 2. Базові питання управління ІБ

Сутність та функції управління. Принципи, підходи та види управління. Цілі і завдання управління ІБ. Поняття системи управління. Поняття кіберінцидента / кібератаки.

ТЕМА 3. Область діяльності СУІБ

Поняття галузі діяльності СУІБ. Склад області діяльності (процеси, структурні підрозділи організації, кадри). Опис галузі діяльності (структура і зміст документа). Розслідування кіберінцидентів / кібератак. Розробка політик ІБ при забезпеченні бізнес-процесів. Дотримання політик ІБ при забезпеченні бізнес-процесів.

Змістовний модуль №2

ТЕМА 4. Стандартизація в галузі управління ІБ

Стандартизація у сфері побудови систем управління. Існуючі стандарти та методології з управління ІБ: їх відмінності, сильні і слабкі сторони (на прикладі

сімейства стандартів 1БО/IEC 2700х, СТО БР ІББС-1.0, ISO 17799, ISO 27001, КО/ШС 18044, СБ 25999 та ін).

ТЕМА 5. Серія стандартів ISO/IEC 27000. Історія серії стандартів ISO/IEC 27000

Історія серії стандартів ISO/IEC 27000. ISO/IEC 27002. Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою. ISO/IEC 27003:2010 Інформаційні технології. Методи захисту. Керівництво по застосуванню системи управління захисту інформації. ISO/IEC 27004 Інформаційні технології. Методи захисту. Вимірювання. ISO/IEC 27006 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікації систем управління інформаційною безпекою. Історія стандарту ISO/IEC 27001.

ТЕМА 6. Система управління ризиками на вимогу стандарту ISO/IEC 27001:2005. Додаток А стандарту ISO/IEC 27001:2005

Технології оцінки та аналізу ризиків. Попередній аналіз та оцінка інформаційних ресурсів організації. ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки. Реалізація вимог стандарту. Засоби управління. Відповідальність керівництва. Методика впровадження системи управління інформаційною безпекою. Документація системи управління інформаційною безпекою.

ТЕМА 7. Системний підхід в управлінні системами менеджменту інформаційної безпеки. Інтеграція системи управління інформаційною безпекою та системи менеджменту якості

Модель PDCA. Додаток В стандарту ISO/IEC 27001:2005. Технологія керування системами менеджменту інформаційної безпеки. Оцінка рівня загроз та уразливостей. Методи вирішення багатокритеріальних завдань управління системами менеджменту інформаційною безпекою. Інтеграція системи менеджменту інформаційної безпеки за вимогами ISO/IEC 27001 та системи менеджменту якості за вимогами ISO 9001:2000. Додаток С стандарту ISO/IEC 27001.

Модуль 2
Змістовний модуль №3

ТЕМА 8. Ризикологія ІБ

Основні визначення та положення ризикології. Мета процесу аналізу ризиків ІБ. Етапи та учасники процесу аналізу ризиків ІБ.

ТЕМА 9. Аналіз ризиків ІБ

Методики аналізу ризиків ІБ. Інвентаризація активів. Поняття активу. Типи активів. Джерела інформації про активи організації.

Визначення загроз ІБ і вразливостей для виділених на етапі інвентаризації активів. Оцінка ризиків ІБ. Планування заходів по обробці виявлених ризиків ІБ.

Затвердження результатів аналізу ризиків ІБ у вищого керівництва. Використання результатів аналізу ризиків ІБ.

ТЕМА 10. Методика оцінки ризиків інформаційної безпеки компанії Digital Security

Метод оцінки ризиків на основі моделі загроз і вразливостей. Основні поняття та припущення моделі. Принцип роботи алгоритму. Вхідні дані: ресурси; критичність ресурсу; відділи, до яких належать ресурси; загрози, що діють на ресурси; уразливості, через які реалізуються загрози; ймовірність реалізації загрози через дану вразливість; критичність реалізації загрози через дану вразливість.

Змістовний модуль №4

ТЕМА 11. Основні процеси СУІБ. Обов'язкова документація СУІБ

Процеси «Управління документами» та «Управління записами» (цілі і завдання процесів, вхідні/вихідні дані, ролі учасників, обов'язкові етапи процесів, зв'язку з іншими процесами СУІБ).

Процеси поліпшення СУІБ («Внутрішній аудит», «Коригувальні дії», «Запобіжні дії»). Процес «Моніторинг ефективності» (включаючи розробку показників ефективності). Поняття «Зрілість процесу». «Аналіз з боку вищого керівництва». Процес «Навчання і забезпечення обізнаності».

ТЕМА 12. Впровадження розроблених процесів. Документ «Положення про застосовність»

Етапи впровадження процесів та їх послідовність. Навчання співробітників, як один з етапів впровадження. Складності, які виникають при впровадженні процесів управління ІБ, і способи їх вирішення. Контроль над впровадженням процесів.

Документування процесу впровадження розроблених процесів. Типовий документ «Положення про застосовність». Мета документа. Структура і зміст документа. Процес розробки документа, рішення спірних ситуацій при розробці документа.

ТЕМА 13. Аудит систем управління інформаційною безпекою. Вимоги стандарту ISO 19011 до проведення аудитів.

Необхідність проведення аудиту систем управління інформаційною безпекою. Етапи внутрішнього аудиту систем управління інформаційною безпекою. Планування та підготовка, програма, тривалість і область діяльності аудиту систем управління інформаційною безпекою. Планування та підготовка аудиту систем управління інформаційною безпекою. Програма, тривалість і область діяльності аудиту систем управління інформаційною безпекою. Техніка аудиту. Алгоритм збору об'єктивних даних у процесі аудиту. Проведення коригувальних та попереджувальних дій. Вимоги до аудиторів. Етика аудиту. Рекомендації аудиторам.

ТЕМА 14. Сертифікація систем управління інформаційною безпекою. Проведення коригувальних та попереджувальних дій. Супровід систем управління інформаційною безпекою.

Організація сертифікаційного аудиту. Вибір організації для сертифікації. Організація перед сертифікаційного аудиту. Організація сертифікаційного аудиту. Консультаційні послуги з виконання коригувальних та попереджувальних дій щодо усунення зауважень, отриманих на перед сертифікаційного аудиті. Супровід систем управління інформаційною безпекою після сертифікаційного аудиту.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	с.р.
1	2	3	4	5	6
Модуль 1					
Змістовий модуль 1. *Базові питання управління інформаційною безпекою*					
Тема 1. Вступ до навчальної дисципліни «Управління інформаційною безпекою»	9	4			5
Тема 2. Базові питання управління ІБ	11	2	4		5
Тема 3. Область діяльності СУІБ	11	2	4		5
Разом за змістовим модулем 1	**31**	**8**	**8**		**15**
Змістовий модуль 2. *Стандарти в галузі управління інформаційною безпекою*					
Тема 4. Стандартизація в галузі управління ІБ	9	2	2		5
Тема 5. Серія стандартів ISO/IEC 27000. Історія серії стандартів ISO/IEC 27000.	9	2	2		5
Тема 6. Система управління ризиками на вимогу стандарту ISO/IEC 27001:2005. Додаток А стандарту ISO/IEC 27001:2005.	9	2	2		5
Тема 7. Системний підхід в управлінні системами менеджменту інформаційної безпеки. Інтеграція системи управління інформаційною безпекою та системи менеджменту якості.	9	2	2		5
Разом за змістовим модулем 2	**36**	**8**	**8**		**20**
Усього годин	**67**	**16**	**16**		**35**
Модуль 2					
Змістовий модуль 3. *Аналіз і оцінка ризиків*					
Тема 8. Ризикологія ІБ	10	3	3		4
Тема 9. Аналіз ризиків ІБ	10	2	3		5
Тема 10. Методика оцінки ризиків інформаційної безпеки компанії Digital Security	10	3	2		5
Індивідуальне завдання	6				6
Разом за змістовим модулем 3	**36**	**8**	**8**		**20**

1	2	3	4	5	6
Змістовий модуль 4. *Впровадження сертифікація та аудит СУІБ*					
Тема 11. Основні процеси СУІБ. Обов'язкова документація СУІБ	9	2	2		5
Тема 12. Впровадження розроблених процесів. Документ «Положення про застосовність»	7	2	2		3
Тема 13. Аудит систем управління інформаційною безпекою. Вимоги стандарту ISO 19011:2002 до проведення аудитів	7	2	2		3
Тема 14. Сертифікація систем управління інформаційною безпекою. Проведення коригувальних та попереджувальних дій. Супровід систем управління інформаційною безпекою.	9	2	2		5
Разом за змістовим модулем 4	**32**	**8**	**8**		**16**
Усього годин	**68**	**16**	**16**		**36**
Усього за дисципліну	**135**	**32**	**32**		**71**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
...	*Не передбачено*	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Дослідження можливості оцінки надійності паролів користувачів систем управління ІБ.	4
2	Дослідження можливості управління функціями ІБ через реєстр.	4
3	Дослідження можливості реалізації програмних методів гарантованого знищення даних з HDD.	4
4	Дослідження можливості реалізації програмних методів відновлення даних з HDD.	5
5	Дослідження можливості оцінки можливості підбору паролю до систем управління ІБ.	4
6	Дослідження можливості реалізації програмних методів відновлення даних з SSD.	5
7	Дослідження та реалізація методики аналізу ризиків корпорації Microsoft.	6

	Разом	**32**

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	2	3
	Не передбачено	

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Опрацювати: Міжнародний стандарт ISO/IEC 27000:2018 Information technology Security techniques. Information security management systems. Overview and vocabulary.	10
2	Опрацювати: Міжнародний стандарт ISO/IEC 27002:2013 Information technology Security techniques. Code of practice for information security controls.	14
3	Ознайомитись з методиками оцінки ризиків, що використовуються на підприємствах України.	15
4	Опрацювати: Методика оцінки ризиків інформаційної безпеки компанії Digital Security на основі інформаційних потоків.	10
5	Опрацювати: стандарт ISO 19011:2002 до проведення аудитів.	10
6	Ознайомитись з міжнародними стандартами серії BSI 17999	6
7	Індивідуальне завдання	6
	Разом	**71**

9. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
1	Побудова моделі інформаційних потоків, моделі загроз та оцінка ризиків на підприємстві.	6

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді екзамену.

12. Розподіл балів, які отримують студенти

12. Критерії оцінювання та розподіл балів, які отримують студенти

12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1			
Робота на лабораторних заняттях. Відмічається активність при виконанні завдань.	0…1	1	0…1
Виконання і захист лабораторних робіт. Своєчасність та виконання всіх завдань лабораторної роботи оцінюється у максимальну оцінку 6 балів.	0...6	1	0...6
Модульний контроль складається з трьох блоків: перший блок – розгорнута відповідь на одне питання (максимум 3 балів), другий блок – п’ять тестових питань по 1 балу, третій блок – п’ять визначень по 2 бали.	0…18	1	0…18
Змістовий модуль 2			
Робота на лабораторних заняттях. Відмічається активність при виконанні завдань.	0…1	1	0…1
Виконання і захист лабораторних робіт. Своєчасність та виконання всіх завдань лабораторної роботи оцінюється у максимальну оцінку 6 балів.	0...6	1	0...6
Модульний контроль складається з трьох блоків: перший блок – розгорнута відповідь на одне питання (максимум 3 балів), другий блок – п’ять тестових питань по 1 балу, третій блок – п’ять визначень по 2 бали.	0…18	1	0…18
Змістовий модуль 3			
Робота на лабораторних заняттях. Відмічається активність при виконанні завдань.	0…1	1	0…1
Виконання і захист лабораторних робіт. Своєчасність та виконання всіх завдань лабораторної роботи оцінюється у максимальну оцінку 6 балів.	0...6	1	0...6
Модульний контроль складається з трьох блоків: перший блок – розгорнута відповідь на одне питання (максимум 3 балів), другий блок – п’ять тестових питань по 1 балу, третій блок – п’ять визначень по 2 бали.	0…18	1	0…18
Змістовий модуль 4			
Робота на лабораторних заняттях. Відмічається активність при виконанні завдань.	0…1	1	0…1
Виконання і захист лабораторних робіт. Своєчасність та виконання всіх завдань лабораторної роботи оцінюється у максимальну оцінку 6 балів.	0...6	1	0...6

Модульний контроль складається з трьох блоків: перший блок – розгорнута відповідь на одне питання (максимум 3 балів), другий блок – п’ять тестових питань по 1 балу, третій блок – п’ять визначень по 2 бали.	0…18	1	0…18
Усього за семестр			**0…100**

Білет для іспиту складається з одного теоретичного та одного практичного запитань, максимальна кількість за кожне із запитань, складає 50 балів.

Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60 – 74). Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи та домашні завдання. Захистити всі індивідуальні завдання та здати тестування.

Добре (75 – 89). Твердо знать мінімум знань, виконати всі завдання. Показати вміння виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах.

Відмінно (90 – 100). Повно знати основний та додатковий матеріал. Знати всі теми. Орієнтуватися у підручниках та посібниках. Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх. Безпомилково виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: httpshttps://mentor.khai.edu/course/view.php?id=3718, на якому розміщено навчально-методичний комплекс дисципліни, який включає в себе:

– робоча програма дисципліни;

– конспект лекцій (презентації), в тому числі в електронному вигляді, який за змістом повністю відповідає робочій програмі дисципліни;

– журнал успішності.

– Посилання на практики

14. Рекомендована література

1. Домарєв В. В., Швець В. А., Шестакова В. В. Організаційне забезпечення захисту інформації з обмеженим доступом: Навчальний посібник. / Національний авіаційний університет; МОН. – К.: НАУ, 2006. – 108 с.
2. Основи управління інформаційною безпекою: навч. посібник /А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.
3. Управління інформаційною безпекою. Конспект лекцій [Електронний ресурс] : навчальний посібник для студентів спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1,11 Мбайт). – Київ:КПІ ім. Ігоря Сікорського, 2021. – 258 с.
4. Управління інформаційною безпекою: навчально-методичний посібник./ А. І. Поворознюк, О.А. Поворознюк – Харків: НТУ «ХПІ», 2021. – 135 с.
5. Управління інформаційною безпекою. Конспект лекцій: навчальний посібник для студентів спеціальності 125 «Кібербезпека» / С. О. Носок, О. М. Фаль, В. М. Ткач. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.
6. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навчальний посібник. / МОН. – К.: Кондор, 2008. – 383 с.
7. Mastering Information Security Compliance Management: A comprehensive handbook on ISO/IEC 27001: 2022 compliance.
8. Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement Hardcover – Illustrated, March 30 2009 by W. Krag Brotby CISM.

Стандарти

1. Міжнародний стандарт ISO 27001 ISO/IEC 27001 Information technology Security techniques. Information security management systems. Requirements.
2. Міжнародний стандарт ISO/IEC 27000 Information technology Security techniques. Information security management systems. Overview and vocabulary.
3. Міжнародний стандарт ISO/IEC 27002 Information technology Security techniques. Code of practice for information security controls.

15. Інформаційні ресурси

1. Державна служба спеціального зв'язку та захисту інформації України [Электрон. ресурс]. - Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/index
2. Міжнародна організація зі стандартизації [Электрон. ресурс]. - Режим доступу: https://www.iso.org/isoiec-27001-information-security.html