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 2021 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 2021 рік

Розробник: Пєвнєв В.Я., доцент кафедри 503, к.т.н., доцент _____
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Цуранов М.В., ст. викладач кафедри 503 _____
(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 « 30 » 08 2021 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 – 4.0</td><td rowspan="11">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>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 4</td><td>2021/2022</td></tr>
<tr><td>Індивідуальне завдання: РГР</td><td rowspan="2">Семестр: 7-й</td></tr>
<tr><td>Загальна кількість годин – 48/120</td></tr>
<tr><td rowspan="7">Кількість тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи студента – 4</td><td>Лекції *.</td></tr>
<tr><td>32 годин</td></tr>
<tr><td>Практичні, семінарські *</td></tr>
<tr><td>16 годин</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>72 годин</td></tr>
<tr><td>Індивідуальні завдання</td></tr>
<tr><td>6 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:
Для денної форми навчання – 48/120.

*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, з: 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.

Компетентності, які набуваються:

- здатність застосовувати знання у практичних ситуаціях.
- знання та розуміння предметної області та розуміння професії.
- здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
- вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
- здатність до пошуку, оброблення та аналізу інформації.
- здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
- здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
- здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
- здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
- здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
- здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
- здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

- здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки.
- здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
- здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Очікувані результати навчання:

- організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
- аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
- адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
- розробляти моделі загроз та порушника;
- 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;
- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
- впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
- 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;
- 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;
- здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;

- застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
- вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
- вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.

Пререквізити – дисципліна є обов'язковим компонентом освітній програми і базується на «Системи технічного захисту інформації», «Безпека операційних систем».

Кореквізити – «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. Наука управління. Принципи, підходи та види управління. Цілі і завдання управління ІБ. Поняття системи управління.

ТЕМА 3. Область діяльності СУІБ

Поняття галузі діяльності СУІБ. Механізм вибору сфери діяльності. Склад області діяльності (процеси, структурні підрозділи організації, кадри). Опис галузі діяльності (структура і зміст документа).

Змістовний модуль №2

ТЕМА 4. Стандартизація в галузі управління ІБ

Стандартизація у сфері побудови систем управління. Історія розвитку. Існуючі стандарти та методології з управління ІБ: їх відмінності, сильні і слабкі сторони (на прикладі сімейства стандартів 1БО/1ЕС 2700х, СТО БР ІББС-1.0, ТОСТ Р ІСО/МЕК 17799, ГОСТ Р ІСО/МЕК 27001,КО/ШС 18044, СБ 25999 та ін).

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

Ресурси як основні об'єкти стандарту. Серія стандартів ISO/IEC 27000. Історія серії стандартів ISO/IEC 27000. SO/IEC 27002:2005 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 27004:2009 Інформаційні технології. Методи захисту. Вимірювання. ISO/IEC 27006:2007 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

Принципи QECD та 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 27001:2005 та системи менеджменту якості за вимогами ISO 9001:2000. Додаток С стандарту ISO/IEC 27001:2005.

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 уразливість; критичність реалізації загрози через дану уразливість.

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 19011:2002 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	**7**	**2**			**5**
Тема 3. Область діяльності СУІБ	**11**	**2**	**4**		**5**
Разом за змістовим модулем 1	**27**	**8**	**4**		**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.	**7**	**2**			**5**
Тема 7. Системний підхід в управлінні системами менеджменту інформаційної безпеки. Інтеграція системи управління інформаційною безпекою та системи менеджменту якості.	**7**	**2**			**5**
Разом за змістовим модулем 2	**32**	**8**	**4**		**20**
Усього годин	**59**	**16**	**8**		**35**
Модуль 2					
Змістовий модуль 3. *Аналіз і оцінка ризиків*					
Тема 8. Ризикологія ІБ	**8**	**3**			**5**

1	2	3	4	5	6
Тема 9. Аналіз ризиків ІБ	**9**	**2**	**2**		**5**
Тема 10. Методика оцінки ризиків інформаційної безпеки компанії Digital Security	**11**	**3**	**2**		**6**
РГР	**6**				**6**
Разом за змістовим модулем 3	**34**	**8**	**4**		**22**
Змістовий модуль 4. *Впровадження сертифікація та аудит СУІБ*					
Тема 11. Основні процеси СУІБ. Обов'язкова документація СУІБ	**7**	**2**			**5**
Тема 12. Впровадження розроблених процесів. Документ «Положення про застосовність»	**4**	**2**			**2**
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	**27**	**8**	**4**		**15**
Усього годин	**61**	**16**	**8**		**37**
Усього за дисципліну	**120**	**32**	**16**		**72**

5. Теми семінарських занять

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

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Отримання практичних навичок оцінки надійності паролів користувачів систем управління ІБ.	2
2	Отримання практичних навичок управління функціями ІБ через реєстр.	2
3	Отримання практичних навичок реалізації програмних методів гарантованого знищення даних з HDD.	2
4	Отримання практичних навичок реалізації програмних методів відновлення даних з HDD.	2
5	Отримання практичних навичок оцінки можливості підбору паролю до систем управління ІБ.	2

6	Отримання практичних навичок реалізації програмних методів відновлення даних з SSD.	2
7	Отримання практичних навичок методики аналізу ризиків корпорації Microsoft.	4
	Разом	**16**

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.	15
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	РГР	6
	Разом	**72**

9. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
1	РГР: 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 іспиту.

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
модуль 1			
Лекції	0…1	8	0…8
Практичні роботи	0...4	3	0…12
Модульний контроль	0…25	1	0..25
модуль 2			
Лекції	0…1	8	0…8
Практичні роботи	0…3	4	0…12
Модульний контроль	0…25	1	0…25
РГР	0…10	1	0…10
Усього за семестр			**0…100**

Контроль знань при проведенні занять оцінюється за такими шкалами:

активність на лекції під час відповідей на питання:

- повна відповідь на питання - 1 бал;
- неповна відповідь – 0,5 бала;
- відсутність на лекції - 0 балів,

виконання і захист практичних робіт:

при виконанні всіх вимог завдань методик на роботи - 4 бали;

- неповні відповіді на питання при захисті результатів роботи за змістом досліджуваної теми - 3 бали;
- неповні відповіді на питання за змістом і результатами роботи - 2 бала;
- недооформлені результати роботи і неповні відповіді на питання за змістом результатів роботи -1балл;
- якщо робота не виконана і не захищена - 0 балів.

На модульний контроль (всього 25 балів) виносяться всі пройдені за контрольований період теми, які включаються в варіанти завдань, що містять по 25 питанньь (по всім темам та видам занять). Максимальна кількість балів за кожне питання - 1.

Семестровий контроль у вигляді іспиту проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних та одного практичного запитань, максимальна кількість за кожне із запитань, складає 33 балу.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 80% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняних та міжнародних стандартів для проведення наукових робіт та робіт щодо захисту інтелектуальної власності.

Добре (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 90% завдань практичних занять. Уміти використовувати сучасні методи теоретичних та експериментальних досліджень для організації та проведення наукових робіт. Мати необхідний обсяг вмінь для одержання позитивної оцінки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Уміти виконувати інформаційне забезпечення наукових досліджень.

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

1. Презентації лекцій.
2. Керівництво до практичних робіт.

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. Сердюк В.А. Организация и технология защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В. А. Сердюк ; Государственный университет - Высшая школа экономики .— Москва : ГУ ВШЭ, 2011. 573 с.
3. Анисимов А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов ; Интернет-университет информациионных технологий .— Москва : ИНТУИТ : БИНОМ. Лаб. знаний, 2010. 175 с.
4. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навчальний посібник. / МОН. – К.: Кондор, 2008. 383 с.

Стандарти

1. Міжнародний стандарт ISO 27001 ISO/IEC 27001:2013 Information technology Security techniques. Information security management systems. Requirements.
2. Міжнародний стандарт ISO/IEC 27000:2018 Information technology Security techniques. Information security management systems. Overview and vocabulary.
3. Міжнародний стандарт ISO/IEC 27002:2013 Information technology Security techniques. Code of practice for information security controls.

15. Інформаційні ресурси

1. Методи захисту програмного забезпечення [Электрон. ресурс]. - Режим доступу: http://www.solon-press/ ru
2. Книги з інформаційної безпеки [Электрон. ресурс]. - Режим доступу: http://bookash.pro/ru/s/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B5+%D0%B2%D0%B8%D1%80%D1%83%D1%81%D1%8B/
3. Державна служба спеціального зв'язку та захисту інформації України [Электрон. ресурс]. - Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/index
4. Міжнародна організація зі стандартизації [Электрон. ресурс]. - Режим доступу: https://www.iso.org/isoiec-27001-information-security.html