МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
_____
Микола АФАНАСЬЄВ

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Кібербезпека***

Статус дисципліни	***базова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Сергій ЄВСЕЄВ*

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 2 від 31.08.2020 р.

Розробник:
Євсеєв С. П., д.т.н., проф. кафедри КІТ.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Дисципліна “Менеджмент інформаційної безпеки” складається з двох модулів, в рамках першого розглядається можливість створення ефективного управління інцидентами інформаційної безпеки за вимогами міжнародних стандартів за рахунок розгляду теоретичних основ менеджменту ІБ, моделі PDCA та етапів ефективного менеджменту інцидентів інформаційної безпеки за вимогами міжнародних стандартів ISO 27035 та ISO 18044. Запропоновані до розгляду особливості менеджменту інцидентів за вимогами міжнародного стандарту ITIL, поняття групи реагування на інциденти ІБ (CERT/CSIRT), інструментарій для ефективного функціонування груп реагування на інциденти ІБ.

В рамках другого модуля дисципліни розглянуті можливі постановки задач аналізу інформаційних ризиків та управління ними при організації режиму інформаційної безпеки в компаніях. Розглянута міжнародна концепція забезпечення інформаційної безпеки, а також різні підходи і рекомендації щодо вирішення завдань аналізу ризиків та управління ними. Дан огляд основних стандартів в галузі захисту інформації та управління ризиками: ISO 17799, ISO 15408, BSI, NIST, MITRE. Наводяться інструментальні засоби для аналізу ризиків (COBRA, CRAMM, MethodWare, RiskWatch). Показаний взаємозв’язок завдань аналізу захищеності і виявлення вторгнень із завданням управління ризиками. Наведені технології оцінки ефективності забезпечення інформаційної безпеки в компаніях.

Метою викладання дисципліни є формування теоретичних знань основних принципів менеджменту управління інцидентами та ризиками на основі вимог міжнародних регуляторів.

Результатами вивчення даної дисципліни є придбання навичок з використання сучасного програмного забезпечення з питань оцінки, аналізу та захисту інформації, яка обробляється в інформаційно-комунікаційних системах від сучасних загроз та інцидентів.

Характеристика навчальної дисципліни

Курс	**2**
Семестр	**4**
Кількість кредитів ECTS	**4**
Форма підсумкового контролю	**залік**

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Інформаційна безпека держави	Інформаційні системи та Інтернет технології
Основи побудови та захисту сучасних операційних систем	Основи математичного моделювання
Введення в мережі	Безпека в інформаційно-комунікаційних системах

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
КЗ 2. Знання та розуміння предметної області та розуміння професії.	РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – 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; РН 5 – адаптуватися в умовах частої зміни технологій професійної

	діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.	РН-9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН-14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН-15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН-16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН-17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН-18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН-20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН-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; РН-35. 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; РН-47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН-50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН-53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН–21вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН–24 вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН–25 забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН–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; РН–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; РН–33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН–34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН–35 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; РН–42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН–43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН–44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН–45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН–46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

Програма навчальної дисципліни

Змістовий модуль 1. Ефективне управління інцидентами інформаційної безпеки за вимогами міжнародних стандартів

Тема 1. *Теоретичні основи менеджменту інформаційної безпеки*

Тема 2. *Модель PDCA опису життєвого циклу процесів управління інцидентами інформаційної безпеки. Етапи ефективного менеджменту інцидентів інформаційної безпеки за вимогами міжнародних стандартів ISO 27035 та ISO 18044*

Тема 3. *Особливості менеджменту інцидентів за вимогами міжнародного стандарту ITIL. Концепція побудови, структура та функціональні особливості ефективної системи менеджменту інцидентів ІБ*
Тема 4. *Поняття групи реагування на інциденти ІБ (CERT / CSIRT): історія розвитку та можливі вигоди перед- прийняттю. Узагальнена класифікація груп CERT / CSIRT: сфера діяльності, цілі та потенційні клієнти*
Тема 5. *Базові етапи створення груп CERT / CSIRT: від визначення середовища існування до співпраці на міжнародному рівні*
Тема 6. *Інструментарій для ефективного функціонування груп реагування на інциденти ІБ. Документаційне забезпечення процесу управління інцидентами ІБ. Діяльність різних груп реагування на інциденти ІБ.*

Змістовий модуль 2. Ризик-менеджмент інформаційної безпеки
Тема 7. *Аналіз ризиків в області захисту інформації*
Тема 8. *Управління ризиками та міжнародні стандарти*
Тема 9. *Технології аналізу ризиків*
Тема 10. *Інструментальні засоби аналізу ризиків*
Тема 11. *Аудит безпеки і аналіз ризиків*
Тема 12. *Виявлення атак і управління ризиками*

Лабораторні роботи
Лабораторна робота 1. *Розгортання операційної системи для проведення аудиту інформаційної безпеки комп'ютерних мереж та систем*
Лабораторна робота 2. *Інструменти прихованого збору технічної інформації з комп'ютерної системи або мережі*
Лабораторна робота 3. *Дослідження вразливостей систем та веб ресурсів за допомогою спеціалізованих сканерів вразливостей (Nessus, Vega)*
Лабораторна робота 4. *Пошук вразливостей та чуттєвої інформації у відкритих ресурсах за допомогою засобу Maltego*
Лабораторна робота 5. *Збір технічної та чуттєвої інформації за допомогою ПЗ класу - сніфери*
Лабораторна робота 6. *Засіб дослідження вразливостей безпровідних мереж Wi-Fi – Aircrack-ng*
Лабораторна робота 7. *Збір інформації за допомогою Metasploit*

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються проблемні лекції, презентації, бесіди, індивідуальні та групові проєкти, майстер-класи.

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних, лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

2) підсумковий/семестровий контроль, що проводиться у формі заліку, відповідно до графіку навчального процесу.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

- вміння впроваджувати процеси, що базуються на стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти кібербезпеки;
- вміння здійснювати оцінювання можливості реалізації загроз в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз;
- вміння аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в системах в ході проведення випробувань згідно встановленої політики кібербезпеки;
- вміння застосовувати національні та міжнародні регулюючі акти в сфері кібербезпеки для розслідування інцидентів;
- вміння здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

За дисципліною передбачені такі методи поточного нормативного оцінювання: опитування та усні коментарі викладача за його результатами, настанови викладачів в процесі виконання лабораторних завдань, формування навичок самооцінювання та обговорення студентами виконаних лабораторних завдань, контроль самостійного виконання індивідуального завдання.

Всі роботи повинні бути виконані самостійно з метою розвитку творчого підходу до рішення задач.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі накопичених балів за виконані поточні та контрольні завдання з лекційних та лабораторних занять, що відображає розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатність творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Практичні (семінарські, лабораторні) заняття: максимальна кількість балів становить 75, а мінімальна – 45.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку їх захисту й виконання контрольних робіт з дисципліни, в технологічній карті бали на цій вид робіт не виділені.

Підсумковий контроль: проводиться за накопиченими балами.

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час заліку, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: “60 і більше балів – зараховано”, “59 і менше балів – не зараховано” та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

Форми оцінювання та розподіл балів наведено у таблиці “Рейтинг-план навчальної дисципліни”.

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано

82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано

Рейтинг-план навчальної дисципліни

Тема	Форми та види навчання		Форми оцінювання	Max бал
Тема 1	***Аудиторна робота***			
	Лекція	Проблемна лекція *"Теоретичні основи менеджменту інформаційної безпеки"*	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №1 *"Розгортання операційної системи для проведення аудиту інформаційної безпеки комп'ютерних мереж та систем"*		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 2	***Аудиторна робота***			
	Лекція	Лекція *"Модель PDCA опису життєвого циклу процесів управління інцидентами інформаційної безпеки"*	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №2 *"Інструменти прихованого збору технічної інформації з комп'ютерної системи або мережі"*	Захист лабораторної роботи № 1	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *"Особливості менеджменту інцидентів за вимогами міжнародного стандарту ITIL"*	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №2 *"Інструменти прихованого збору технічної інформації з комп'ютерної системи або мережі"*		
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Лекція	Лекція *"Поняття групи реагування на інциденти ІБ (CERT / CSIRT): історія розвитку та можливі вигоди перед-прийняттю"*	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №3 *"Дослідження вразливостей систем та веб ресурсів за допомогою спеціалізованих сканерів вразливостей (Nessus, Vega"*	Захист лабораторної роботи № 2	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 5	***Аудиторна робота***			
	Лекція	Лекція *"Базові етапи створення груп CERT / CSIRT: від визначення середовища існування до співпраці на міжнародному рівні"*	Експрес-опитування	2
	Лабораторне заняття	Лабораторна робота №3 *"Дослідження вразливостей систем та веб ресурсів за допомогою спеціалізованих сканерів вразливостей (Nessus, Vega"*	Контрольна робота 1	20
Тема 6	***Аудиторна робота***			
	Лекція	Лекція *"Інструментарій для ефективного функціонування груп реагування на інциденти ІБ"*	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №4. *"Пошук вразливостей та чуттєвої інформації у відкритих ресурсах за допомогою засобу Maltego"*	Захист лабораторної роботи № 3	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену		
Тема 7	***Аудиторна робота***			
	Лекція	Лекція *"Аналіз ризиків в області*	Робота на	2

		захисту інформації"	лекції	
	Лабораторне заняття	Лабораторна робота №5. *"Збір технічної та чуттєвої інформації за допомогою ПЗ класу - сніфери"*	Захист лабораторної роботи № 4	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція *"Управління ризиками та міжнародні стандарти"*	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №5. *"Збір технічної та чуттєвої інформації за допомогою ПЗ класу - сніфери"*		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену		
Тема 9	***Аудиторна робота***			
	Лекція	Лекція *"Технології аналізу ризиків"*	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №6. *"Засіб дослідження вразливостей безпровідних мереж Wi-Fi – Aircrack-ng"*	Захист лабораторної роботи № 5	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену		
Тема 10	***Аудиторна робота***			
	Лекція	Лекція *"Інструментальні засоби аналізу ризиків"*	Експрес-опитування	2
	Лабораторне заняття	Лабораторна робота №6. *"Засіб дослідження вразливостей безпровідних мереж Wi-Fi – Aircrack-ng"*		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену:		

		виконання типових завдань за теорією		
Тема 11	***Аудиторна робота***			
	Лекція	Лекція *"Аудит безпеки і аналіз ризиків"*	Робота на лекції	2
	Лабораторне заняття	Лабораторна робота №7. *"Збір інформації за допомогою Metasploit"*	Захист лабораторної роботи № 6	5
			Контрольна робота 2	20
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену: виконання типових завдань за практичною складовою		
Тема 12	***Аудиторна робота***			
	Лекція	Лекція *"Виявлення атак і управління ризиками"*	Робота на лекції	3
	Лабораторне заняття	Лабораторна робота №7. *"Збір інформації за допомогою Metasploit"*	Захист лабораторної роботи № 7	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань. Підготовка до екзамену: виконання типових завдань за практичною складовою		

Рекомендована література

Основна

1. Р. В. Грищук, та Ю. Г. Даник. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016.

2. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. – М. : Академия АйТи : ДМК Пресс, 2008. – 384 с.

3. О. Г. Корченко, О. Є. Архипов, та Ю. О. Дрейс, "Оцінювання шкоди національній безпеці України у разі витоку державної таємниці", монографія, К: наук.-вид.центр НА СБУ України, 2014.

4. Аудит та управління інцидентами інформаційної безпеки: навч. посіб.

[Електронний ресурс] / [КорченкоО.Г., Гнатюк С.О., КазмірчукС.В. та ін.]. –К.: Центр навч.-наук. та наук.-пр. видань НАСБ України, 2014. – 190 с. – Режим доступу:

http://193.178.34.24/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf .

Додаткова

5. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

6. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів національного банку України/ [Електронний ресурс]. Доступно: zakon.rada.gov.ua/laws/show/v0365500-11.

7. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Электронный ресурс]. Доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11423.

8. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій. [Электронный ресурс]. Доступно: http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekoiu-informatsiinikh-tiekhnologhii. Дата звернення: Груд. 7.2017.

9. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій. [Электронный ресурс]. Доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11425.

10. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту. [Электронный ресурс]. Доступно: http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005

11. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою. [Электронный ресурс]. доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11427.

Інформаційні ресурси.

12. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни "Менеджмент інформаційної безпеки" https://pns.hneu.edu.ua/course/view.php?id=4924.