Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«01» 09 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «УПРАВЛІННЯ ІНЦИДЕНТАМИ БЕЗПЕКИ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

2022 – 2023 навчальний рік

Розробник:
Рой Яніна Володимирівна, кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:
Рой Яніна Володимирівна, кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____ Павло СКЛАДАННИЙ
(підпис)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.
Керівник освітньої програми _____ Артем ПЛАТОНЕНКО
(підпис)

Робочу програму перевірено
___.___. 2022 р.
Заступник декана _____ Євген ІВАНІЧЕНКО
(підпис)

Пролонговано:
на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)
на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)
на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)
на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	5 / 150	
Курс	4	
Семестр	7	
Кількість змістових модулів з розподілом:	5	
Обсяг кредитів	5	
Обсяг годин, в тому числі:	150	
Аудиторні	70	
Модульний контроль	10	
Семестровий контроль	-	
Самостійна робота	70	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Управління інцидентами безпеки» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 «Кібербезпека».

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Управління інцидентами безпеки» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Управління інцидентами безпеки» складається з п’ятьох змістових модулів: Аналіз функціональних методів оцінки ризиків кібербезпеки, Оцінка уразливості і ризиків для інформаційних ресурсів, що підлягають захисту, при виявленій множині загроз, Оцінка ризиків на основі експертних методів, Менеджмент інцидентів інформаційної безпеки, Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.

Обсяг дисципліни – 150 годин (5 кредитів).

Метою викладання навчальної дисципліни «Управління інцидентами безпеки» є вивчення основних методів та засобів оцінки ризиків та методів управління інцидентами інформаційних ресурсів, які реалізовані у сучасних базових технологіях інформаційної безпеки.

Завдання:

- вивчення теоретичних основ і положень захисту інформації;
- отримання необхідних теоретичних знань побудови систем захисту інформації;
- отримання практичних навиків оцінювання ризиків інформаційної безпеки.

У результаті вивчення навчальної дисципліни формуються загальні компетентності:

- ***компетентності у сфері навчання:***
  - здатність до організації самостійної навчальної, практичної та науково-дослідної діяльності;
- ***компетентності у сфері застосування знань в практичних ситуаціях***

- вміння застосовувати здобуті теоретико-концептуальні професійні знання у процесі практичної, викладацької та науково-дослідної роботи;

фахові компетентності:

- ***компетентності у сфері інформаційної безпеки:***
  - 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 забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;.
  - здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності;
  - здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки.
- **компетентності у сфері науково-дослідної діяльності:**
  - уміння вивчати і систематизувати досягнення вітчизняних і зарубіжних досліджень у галузі інформаційно-комунікаційних технологій, педагогіки і психології, суміжних галузей знань;
  - вивчати, узагальнювати й упроваджувати на практиці вітчизняний і зарубіжний досвід управління інформаційними технологіями і системами, інформаційною інфраструктурою тощо.
- **компетентності у сфері вмінь працювати в групі:**
  - здатність використовувати навички взаємодії в роботі, компетентності у сфері навичок міжособистісного спілкування
  - здатність до продуктивного використання комунікації як складової професійної діяльності.

3. Результати навчання за дисципліною

При вивченні курсу «Управління ризиками та інцидентами інформаційної безпеки» студенти повинні

знати:

- методи, методики, програмні засоби оцінки ризиків інформаційної безпеки в ІТС підприємств, установ, організацій;
- модель прийняття рішень оцінки ризиків експертними методами;
- етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035;
- діяльність груп CERT/CSIRT та етапи їх створення;
- документаційне забезпечення процесу управління інцидентами інформаційної безпеки

уміти:

- здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей;
- оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж.
- виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп'ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення,

неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення

- впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки; застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів інформаційної безпеки.
- розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем застосовувати політики, що базуються риск адаптивному контролі доступу; здійснювати аналіз ризиків функціонування ІКС: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками.
- використовувати теоретичні і практичні методи та методики досліджень у галузі інформаційної безпеки; застосовувати системний підхід та знання основ теорії інформаційної безпеки

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Аналіз функціональних методів оцінки ризиків кібербезпеки							
Тема 1. Аналіз стандартів оцінки ризиків та методів управління ризиками інформаційної безпеки	13	2	2	2			7
Тема 2. Порівняння моделей прийняття рішень з інформаційної безпеки	13	2	2	2			7
Модульний контроль	2						
Разом	28	4	4	4			14
Змістовий модуль 2. Оцінка уразливості і ризиків для інформаційних ресурсів, що підлягають захисту, при виявленій множині загроз							
Тема 3. Оцінка вразливості інформаційних ресурсів	13	2	2	2			7
Тема 4. Оцінка ризиків для інформаційних ресурсів	13	2	2	2			7
Модульний контроль	2						
Разом	28	4	4	4			14
Змістовий модуль 3. Оцінка ризиків на основі експертних методів							
Тема 5. Модель прийняття рішень оцінки ризиків експертними методами	13	2	2	2			7
Тема 6. Методика оцінювання інформаційних ризиків в системі управління інформаційною безпекою	13	2	2	2			7
Модульний контроль	2						
Разом	28	4	4	4			14
Змістовий модуль 4. Менеджмент інцидентів інформаційної безпеки							

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Тема 7. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035	13	2	2	2			7
Тема 8. Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки	13	2	2	2			7
Модульний контроль	2						
Разом	28	4	4	4			14
Змістовий модуль 5. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT							
Тема 9. Загальна характеристика діяльності груп CERT/CSIRT та етапи їх створення	16	2	4	4			6
Тема 10. Обробка інцидентів інформаційної безпеки групами CERT/CSIRT	10	2	2	2			4
Тема 11. Документаційне забезпечення процесу управління інцидентами інформаційної безпеки	10	2	2	2			4
Модульний контроль	2						
Разом	38	6	8	8			14
Усього	**150**	**22**	**24**	**24**			**70**

5. Програма навчальної дисципліни

Змістовий модуль1. Аналіз функціональних методів оцінки ризиків кібербезпеки

Основні питання:

- Аналіз стандартів оцінки ризиків та методів управління ризиками інформаційної безпеки.
- Порівняння моделей прийняття рішень з інформаційної безпеки.

Змістовий модуль 2. Оцінка уразливості і ризиків для інформаційних ресурсів, що підлягають захисту, при виявленій множині загроз

Основні питання:

- Оцінка вразливості інформаційних ресурсів.
- Оцінка ризиків для інформаційних ресурсів.

Змістовий модуль 3. Оцінка ризиків на основі експертних методів

Основні питання:

- Модель прийняття рішень оцінки ризиків експертними методами.
- Методика оцінювання інформаційних ризиків в системі управління інформаційною безпекою

<u>Змістовий модуль 4</u>. Менеджмент інцидентів інформаційної безпеки

Основні питання:

- Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035.
- Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки.

<u>Змістовий модуль 5</u>. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT

Основні питання:

- Загальна характеристика діяльності груп CERT/CSIRT та етапи їх створення
- Обробка інцидентів інформаційної безпеки групами CERT/CSIRT
- Документаційне забезпечення процесу управління інцидентами інформаційної безпеки

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен.
- *Комп'ютерного контролю:* тестові програми.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4		Модуль 5	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	2	2	2	2	2	2	2	2	3	3
Відвідування семінарських занять	1	2	2	2	2	2	2	2	2	4	4
Відвідування практичних занять	1	2	2	2	2	2	2	2	2	4	4
Відвідування лабораторних занять	1										
Робота на семінарському занятті	10	2	20	2	20	2	20	2	20	4	40
Робота на практичному занятті	10	2	20	2	20	2	20	2	20	4	40
Лабораторна робота (в тому числі допуск, виконання, захист)	10										
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25	1	25	1	25
Виконання ІНДЗ	30										
Разом		-	76	-	76	-	76	-	76	-	121
Максимальна кількість балів: 425											
Розрахунок коефіцієнта: 425/100=4,25											

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль1. Аналіз функціональних методів оцінки ризиків кібербезпеки		**14**	**5**
1	Виявлення повної множини загроз безпеки інформаційним ресурсам, які підлягають захисту.	14	5
Змістовий модуль 2. Оцінка уразливості і ризиків для інформаційних ресурсів, що підлягають захисту, при виявленій множині загроз		**14**	**5**
2	Проведення оцінки уразливості та ризиків для інформаційних ресурсів, що підлягають захисту, при виявленій множині загроз	14	5
Змістовий модуль 3. Оцінка ризиків на основі експертних методів		**14**	**5**
3	Визначення інформаційних ресурсів, що підлягають захисту	14	5
Змістовий модуль 4. Менеджмент інцидентів інформаційної		**14**	**5**

№ з/п	Назва теми	Кількість годин	Бали
безпеки			
4	Активний аудит інформаційних систем	14	5
<u>Змістовий модуль 5</u>. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT		**14**	**5**
5	Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035	14	5
Разом		**70**	**25**

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп'ютерний тест, що складається 20 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі заліку, умовою отримання якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Шкала відповідності оцінок

Рейтингова оцінка	Сума балів за всі види навчальної діяльності	Значення оцінки
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов'язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 150 год., лекції – 22 год., семінарські заняття – 24 год., практичні роботи – 24 год., модульний контроль – 10 год., самостійна робота –70 год.

Модулі (назви, бали)	**Змістовий модуль 1** Аналіз функціональних методів оцінки ризиків кібербезпеки (76 балів)		**Змістовий модуль 2** Оцінка уразливості і ризиків для інформаційних ресурсів, що підлягають захисту, при виявленій множині загроз (76 балів)		**Змістовий модуль 3** Оцінка ризиків на основі експертних методів (76 балів)		**Змістовий модуль 4** Менеджмент інцидентів інформаційної безпеки (76 балів)		**Змістовий модуль 5** Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT (121 бал)		
Лекції (теми, бали)	Аналіз стандартів оцінки ризиків та методів управління ризиками інформаційної [illegible]	Порівняння моделей прийняття рішень з інформаційної безпеки (1 бал)	Оцінка вразливості інформаційних ресурсів (1 6бал)	Оцінка ризиків для інформаційних ресурсів (1 бал)	Модель прийняття рішень оцінки ризиків експертними методами (1 бал)	Методика оцінювання інформаційних ризиків в системі управління інформаційною безпекою (1 бал)	Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035 (1 бал)	Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки (1 бал)	Загальна характеристика діяльності груп CERT/CSIRT та етапи їх створення (1 бал)	Обробка інцидентів інформаційної безпеки групами CERT/CSIRT (1 бал)	Документаційне забезпечення процесу управління інцидентами інформаційної безпеки (1 бал)
Практичні заняття (теми, бали)	Ризик порушення поточної технології (11 балів)	Методи математичного програмування для визначення оптимальної виробничої програми [illegible]	Ризик порушення поточної технології виробництва (11 балів)	Мінімаксна оцінка ризику (11 балів)	Визначення поняття ймовірність події(11 балів)	Якісний і кількісний аналіз небезпек (11балів)	Імовірнісний розрахунок надзвичайної події (11балів)	Оцінка випуску в оболонці LabVIEW (11 бали)0 балів)	Оцінка і керування ризиками. Метод VAR (22 бали)	Теоретичні відомості щодо керування ризиками методом «Value at Risk (VAR) - Сума під ризиком » (10 балів)	управління ризиками, управління якістю й відстеження зв'язків. (11 балів)
Семінарські заняття (теми, бали)	Ризик порушення поточної технології (11 балів)	Методи математичного програмування для визначення оптимальної виробничої програми (11 балів)	Ризик порушення поточної технології виробництва (11 балів)	Мінімаксна оцінка ризику (11 балів)	Визначення поняття ймовірність події(11 балів)	Якісний і кількісний аналіз небезпек (11 балів)	Імовірнісний розрахунок надзвичайної події (11 балів)	Оцінка випуску в оболонці LabVIEW (11 бали)0 балів)	Оцінка і керування ризиками. Метод VAR (22 бали)	Теоретичні відомості щодо керування ризиками методом «Value at Risk (VAR) - Сума під ризиком » (11балів)	управління ризиками, управління якістю й відстеження зав'язків. (11 балів)
Самостійна робота	Самостійна робота (5 балів)		Самостійна робота (5 балів)		Самостійна робота (5 балів)		Самостійна робота (5 балів)		Самостійна робота (5 балів)		
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)		Модульна контрольна робота 2 (25 балів)		Модульна контрольна робота 3 (25 балів)		Модульна контрольна робота 4 (25 балів)		Модульна контрольна робота 5 (25 балів)		
Підсумковий контроль (вид, бали)	Залік										

8. Рекомендовані джерела

Основна (базова):

1. Єсін В.І., Кузнєцов А.А., Сорока Л.С. Безпека інформаційних систем та технологій – Х.: «ЕДЕНА», 2010. – 656с.
2. Горбенко І.Д., Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації – Харків: ХНУРЕ, 2004 – 368 с.
3. Домарев В.В. Безпека інформаційних технологій: Системний підхід. – К.: "ТІД ДС", 2004. – 992с.

Додаткова

1. Гарасим Ю.Р. Аналіз систем захисту, які мають властивість живучості / Ю. Р. Гарасим // Військово-технічний збірник. – 2016. № 1 (4). – С. 87–95.
2. Гарасим Ю.Р. Забезпечення живучості та неперервності функціонування систем захисту інформації / Ю. Р. Гарасим, В. А. Ромака, М. М. Рибій // Вісник Нац. ун-ту “Львівська політехніка” “Автоматика, вимірювання та керування”. – 2014. – № 741. – С. 105- 112.
3. Замула О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О.А. Замула, В.І. Черниш // Системи обробки інформації: збірних наукових праць. – Х.: ХУ ПС, 2014. – Вип. 2(92). – С. 53-56.
4. Корченко А.Г. Побудова систем захисту інформації на нечітких множинах. Теорія і практичні рішення – К.: МК-Пресс, 2016. – 324 с.
5. Alberts C. J. Operationally Critical Threat, Asset and Vulnerability Evaluation / C. J. Alberts, S. G. Behrens, R. D. Pethia, W. R. Wilson. – 2018. – P. 84.
6. Endorf C. F. Measuring ROI on security / Carl F. Endorf // Information security management handbook / Edited by Harold F. Tipton and Micki Krauze. – 6th edition. – Boca Raton: Auerbach Publications, 2017. – Part 1, Section 1.1, Ch. 12. – P. 133-137.
7. Henry K. Risk management and analysis / Kevin Henry // Information Security Management Handbook / Edited by Harold F. Tipton, Micki Krauze. – 6th edition. – Boca Raton : Auerbach Publications, 2017. – Part 1, Section 1.4, Ch. 28. – P. 321-329.
8. ISO/IEC 27035. Information technology. Security techniques. Information security incedent management. – 2011. – 78 p.
9. Landoll D. The security risk assessment handbook: a complete guide for performing security risk assessments / Douglas J. Landoll. – Boca Raton: Auerbach Publications, 2016. – 504 p.
10. Rittinghouse J. W. Business continuity and disaster recovery for infosec managers / John W. Rittinghouse, James F. Ransome. – Oxford: Elsevier, 2015. – 408 p.
11. Spedding L. Business risk management handbook: a sustainable approach / Linda Spedding, Adam Rose. – Oxford: Elsevier, 2018. – 768 p.

9. Додаткові ресурси

1. http://ito.vspu.net/Prakt_IT/PIDSUMOK/2014-2015/rob/Klochenok/tzi.html