

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС

нормативної навчальної дисципліни

СИСТЕМИ МОНІТОРИНГУ ЗАГРОЗ

підготовки бакалавра галузі знань 12 «Інформаційні технології»
спеціальності 125 «Кібербезпека» освітньо-професійної програми
«Інформаційна безпека»

Луцьк – 2020

Силабус навчальної дисципліни «Системи моніторингу загроз» підготовки бакалавра, галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека» за освітньо-професійною програмою «Інформаційна безпека»

Розробник: Острей О.Р., старший викладач кафедри комп'ютерних наук та кібербезпеки, інженер з комп'ютерних систем відділу технічних засобів навчання «Центр інноваційних технологій та комп'ютерного тестування»

Силабус навчальної дисципліни затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол №4 від 05 листопада 2020 р.

Завідувач кафедри:



(Гришанович Т.О.)

1. Опис навчальної дисципліни

Таблиця 1

Найменування показників	Галузь знань, спеціальність, освітня програма, освітній ступінь	Характеристика навчальної дисципліни
Денна форма навчання	Шифр і назва галузі знань: 12 «Інформаційні технології» Спеціальність: 125 «Кібербезпека» Освітньо-професійна програма «Інформаційна безпека» Освітній ступінь бакалавр	Нормативна
Кількість годин/кредитів 120/4		Рік навчання 3
ІНДЗ: немає		Семестр_5-ий
Мова навчання		Лекції 24 год.
		Лабораторні 30 год.
		Самостійна робота 57 год.
		Консультації 9 год.
	Форма контролю: іспит	
	українська	

II. Інформація про викладача

ПП: Острей Оксана Ростиславівна

Посада: старший викладач кафедри комп'ютерних наук та кібербезпеки, інженер з комп'ютерних систем відділу технічних засобів навчання «Центр інноваційних технологій та комп'ютерного тестування».

Контактна інформація (номер мобільного зв'язку, електронна адреса): 0508667216, ostrey.oxana@vnu.edu.ua

Дні занять (посилання на електронний розклад):

<http://194.44.187.20/cgi-bin/timetable.cgi?n=700>

III. Опис дисципліни

1. Анотація курсу

Навчальна дисципліна «Системи моніторингу загроз» є нормативною для ОПП «Інформаційна безпека», спрямована на вивчення функцій, задач та принципів моніторингу, систем моніторингу загроз різного виду. У курсі розглядається основні теоретичні положення організації моніторингу, систем моніторингу. Досліджуються можливі загрози інформаційній безпеці, які виступають об'єктами моніторингу. Розглядається практичне застосування різних засобів та методів моніторингу. Вивчається моделювання систем безпеки та побудова прототипів систем безпеки, на прикладах деяких систем моніторингу загроз. Зміст курсу: Сутність понять «моніторинг», «системи моніторингу». Види загроз інформаційній безпеці. Сутність управління системою інформаційної безпеки. Складові системи управління інформаційною безпекою. Різновиди систем моніторингу загроз інформаційній безпеці у різних сферах.

2. Пререквізити/постреквізити

Пререквізити: Основи комп'ютерної фізики, Комп'ютерна дискретна математика, Прикладна математика в ІТ-галузі, Сучасне програмне забезпечення та хмарні технології, Організація баз даних та знань, Новітні інформаційні технології для аналізу і обробки даних,

Вступ до фаху, Нормативно-правова база кібербезпеки, Організаційне забезпечення захисту інформації, Архітектура комп'ютерних систем та схемотехніка, Теорія ризиків інформаційної безпеки, Проектування мікроконтролерних систем та основи мехатроніки, Діагностика шкідливого програмного забезпечення.

Постреквізити: Технічний захист інформації, Безпека інфраструктури комп'ютерних мереж, Моделювання та безпека соціальних процесів, Комплексні системи захисту інформації, Захист інформації в інформаційно-комунікаційних системах, Технологія програмування захищених систем, Практика технологічна та виробнича.

3. Мета і завдання навчальної дисципліни:

Мета навчальної дисципліни – сформувати у здобувачів систему спеціальних знань з питань організації систем моніторингу загроз інформаційній безпеці.

Завдання:

розглянути основні теоретичні положення організації моніторингу, системмоніторингу; дослідити можливі загрози інформаційній безпеці, які виступають об'єктами моніторингу. ознайомитися з методами та засобами моніторингу та отримати навички їх практичного застосування для проведення моніторингу загроз інформаційній безпеці;

розглянути принципи моделювання систем безпеки та навчитися створювати прототипи систем безпеки на прикладах деяких систем моніторингу загроз;

формувати навички застосування отриманих у навчальній дисципліні знань на практиці та планувати власну кар'єру як аналітиків комп'ютерних систем; менеджерів (управителів) систем з інформаційної безпеки; керівників підрозділу з безпеки; професіоналів із організації інформаційної безпеки.

Методи навчання: лекція, лабораторна робота, усне опитування, письмові контрольні роботи, самостійна робота, індивідуальна робота.

4. Результати навчання (компетентності).

Навчальна дисципліна «Системи моніторингу загроз» надає основні компетентності, якими має володіти здобувач першого рівня вищої освіти за спеціальністю 125 «Кібербезпека»:

1. Здатність застосовувати знання у практичних ситуаціях. (ЗК 1).
2. Знання та розуміння предметної області та розуміння професії. (ЗК 2).
3. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. (ЗК 4)
4. Здатність до пошуку, оброблення та аналізу інформації. (ЗК 5).
5. Здатність здійснювати професійну діяльність на основі впроваджені системи управління інформаційною безпекою та/або кібербезпекою. (ФК 9)
6. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. (ФК 11).
7. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. (ФК 12).
8. 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. (ПРН 4)
9. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. (ПРН 10)
10. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. (ПРН 11)
11. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. (ПРН 51)
12. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. (ПРН 49)

По завершенні вивчення дисципліни студенти будуть компетентними у таких питаннях:

- будувати та спроектувати схему системи моніторингу, визначити об'єкт та методи моніторингу;

- орієнтуватися у спеціалізованих системах моніторингу та їх використанні;
- розрізняти та помічати загрози інформаційній безпеці;
- аналізувати необхідність застосування системи моніторингу загроз інформаційній безпеці.

5. Структура навчальної дисципліни

Назви змістових модулів і тем	Усього	Лекції	Лабораторні	Сам.робота	Консультації	Бали
Змістовий модуль 1. Парадигма "Моніторингу", "Системи моніторингу загроз"						
Тема №1. Основні поняття та концепції моніторингу. Компоненти та рівні систем моніторингу.	4	2		1		2
Тема №2. Побудова схеми управлінського моніторингу конкретного об'єкту	4		2	1		2
Тема №3: Сутність моніторингу в окремих сферах діяльності. Класифікація систем моніторингу	4	2		1	1	2
Тема №4. Функції, задачі та принципи організації моніторингу. (На основі аналізу моніторингових онлайнресурсів)	4		2	2		2
Тема №5. Лекція №3. Загрози інформаційній безпеці як об'єкт моніторингу	4	2		2		2
Тема №6. Поняття, структура, алгоритм розробки Паспорта загрози інформаційній безпеці.			2	2	1	8
Тема №7. Роль державних органів організації системи моніторингу загроз інформаційній безпеці		2		2		2

Тема №8. Датчики, якджерело збору інформації у автоматизованих системах моніторингу. Дослідження принципів роботи датчиків.			2	2	1	2
Тема №9. Засоби збору та зберігання інформації. Бази даних. Системи управління базами даних. Штучний інтелект у системах моніторингу загроз		2		10*		20
Тема №10. Організація відеонагляду та онлайн камери як засіб моніторингу			2	2	1	4
Разом за змістовим модулем 1		10	10	25	4	46
Змістовий модуль 2. Практичне застосування систем моніторингу загроз у конкретних галузях						
Тема №11. Організація систем моніторингу загроз підприємства		2	2	2		4
Тема №12. Системи моніторингу загроз національній безпеці		2	2	2	1	8
Тема №13. Системи моніторингу комп'ютерних мереж, системи виявлення атак (СВА), сканери мережі SIEM, HP Operations Manager, ManageEngine OpManager, SolarWinds, IBM Tivoli, WhatsUp Gold		2	4	4	2	4
Тема №14. Кібергігієна - як основа захисту від загроз в інформаційному суспільстві				10**		20
Тема №15. Системи моніторингу загроз соціально-економічній безпеці		2	2	2		4

Тема №16. Системи моніторингу загроз оборонно- військової галузі		2		2		2
Тема №17. Вивчення реалізації моніторингових функцій Головним центром спеціального контролю та Спеціальної моніторингова місія ОБСЄ в Україні			2	2		2
Тема №18. Безпілотні літаючі апарати як засіб моніторингу			2	2		2
Тема №19. Автоматизовані системи моніторингу. Пристрої управління датчиками, на прикладі Arduino Mega 2560			2	2	1	2
Тема №20. Автоматизовані системи моніторингу, на прикладі систем Smart house та професійної системи безпеки Ажкс		2	2	2	1	2
Тема №2. Інформаційно-аналіт ична технологія моніторингу засобами MicroStrategy Platform			2	2		2
Разом за змістовим модулем 2		14	20	32	5	54
Усього годин	120	24	30	57	9	100

*студенти самостійно освоюють курс: “Штучний інтелект” на онлайн платформі “ДІЯ. Цифрова освіта”. Важливість детального розгляду саме цього курсу полягає у тому, що фактично всі системи моніторингу в модулі опрацювання, аналізу та прогнозування зібраної інформації базуються на принципах функціонування штучного інтелекту (ШІ), нейромереж. Даний курс ознайомить студентів з математичними основами ШІ та принципами його функціонування.

**студенти самостійно освоюють курс “Основи кібергігієни” (для держслужбовців) на онлайн платформі “ДІЯ. Цифрова освіта”. Важливість детального розгляду саме цього курсу полягає у тому, що для запобігання загроз інформаційній безпеці держави основою є дотримання правил кібергігієни кожним членом інформаційного суспільства.

Результатами успішного засвоєння даних курсів є отримання відповідних

сертифікатів. Представлений сертифікат зараховується як результат модульної контрольної роботи, що регламентується Положенням про визнання результатів навчання, отриманих у формальній, неформальній та/або неформальній освіті у Волинському національному університеті імені Лесі Українки (<https://bit.ly/3ujdnxS>).

Тематика лабораторних занять

№ з/п	Тема	Кількість годин
1	Побудова схеми управлінського моніторингу конкретного об'єкту	2 год.
2	Функції, задачі та принципи організації моніторингу (На основі аналізу моніторингових онлайн ресурсів)	2 год.
3	Поняття, структура, алгоритм розробки Паспорта загрози національній безпеці	2 год.
4	Датчики, як джерело збору інформації у автоматизованих системах моніторингу. Дослідження принципів роботи датчиків	2 год.
5	Організація відеонагляду як засібу моніторингу периметру, онлайн камери як засіб моніторингу загроз суспільній безпеці	2 год.
6	Організація політики та систем моніторингу інформаційної безпеки підприємств	2 год.
7	Засоби запобігання загрозам інформаційній безпеці при роботі з мережею "Інтернет"	2 год.
8	Загрози інформаційної безпеки держави в соціальних мережах та месенджерах	2 год.
9	Системи моніторингу комп'ютерних мереж, системи виявлення атак (СВА), сканери мережі: SIEM, HP Operations Manager, ManageEngine OpManager, SolarWinds, IBM Tivoli, WhatsUp Gold	2 год.
10	Механізми моніторингу загроз інформаційній безпеці України соціально-економічного характеру	2 год.
11	Автоматизовані системи моніторингу. Пристрої управління датчиками, на прикладі Arduino Mega 2560	2 год.
12	Автоматизовані системи моніторингу, на прикладі систем Smart house та професійної системи безпеки Аjкс	2 год.
13	Інформаційно-аналітична технологія моніторингу засобами MicroStrategy Platform	2 год.
14	Безпілотні літаючі апарати як засіб моніторингу	2 год.
15	Вивчення реалізації моніторингових функцій Головним центром спеціального контролю та Спеціальної моніторингова місія ОБСЄ в Україні	2 год.
	Всього	30 год

Питання до іспиту

1. Основні поняття: “моніторинг”, “системи моніторингу”.
2. Схема управлінського моніторингу конкретного об'єкту.
3. Складові системи моніторингу.
4. Рівні забезпечення моніторингу.
5. Загрози інформаційній безпеці як об'єкт моніторингу.
6. Сутність моніторингу в окремих сферах діяльності.
7. Класифікація систем моніторингу.
8. Функції та задачі моніторингу.
9. Принципи організації моніторингу.
10. Поняття, структура, алгоритм розробки Паспорта загрози інформаційній безпеці
11. Роль державних органів у організації системи моніторингу загроз інформаційній безпеці.

12. Датчики, як джерело збору інформації у автоматизованих системах моніторингу
13. Принципи роботи датчиків
14. Засоби збору та зберігання інформації у системах моніторингу загроз.
15. Бази даних у системах моніторингу загроз.
16. Штучний інтелект у системах моніторингу загроз
17. Організація відеонагляду та онлайн камери як засіб моніторингу
18. Організація систем моніторингу загроз підприємства
19. Спеціалізовані системи моніторингу: банківський моніторинг.
20. Системи моніторингу загроз інформаційній безпеці
21. Системи моніторингу комп'ютерних мереж, системи виявлення атак (СВА), сканери мережі
22. Кібергігієна - як основа захисту від загроз в інформаційному суспільстві
23. Класифікація загроз національній безпеці.
24. Види загроз інформаційній безпеці.
25. Загрози інформаційної безпеки держави в соціальних мережах.
26. Система моніторингу загроз соціальній безпеці.
27. Система моніторингу загроз економічній безпеці.
28. Система моніторингу загроз інформаційній безпеці.
29. Системи моніторингу загроз оборонно-військової галузі
30. Моніторингові функції Головного центру спеціального контролю
31. Діяльність Спеціальної моніторингової місії ОБСЄ в Україні
32. Безпілотні літаючі апарати як засіб моніторингу
33. Автоматизовані системи моніторингу, на прикладі систем Smart house та Професійна система безпеки Ауах

IV. Політика оцінювання

Здобувач має виконати у повному обсязі усі види діяльності із навчальної дисципліни «Системи моніторингу загроз», бути присутніми на аудиторних заняттях. Якщо здобувач відсутній на занятті, він може надіслати виконане семінарське заняття у письмовому вигляді.

Освітній процес відповідає «Положенню про поточне та підсумкове оцінювання знань студентів Волинського національного університету імені Лесі Українки» від 11 вересня 2020 р. (<https://bit.ly/39In2ac>). Іспит виставляється автоматично за умови, якщо студент виконав усі види навчальної роботи та отримав не менше ніж 75 балів зі 100 можливих.

Вирішення спірних питань у галузі академічної доброчесності здійснюється на підставі Положення про систему запобігання та виявлення академічного плагіату у науково-дослідній діяльності здобувачів вищої освіти і науково-педагогічних працівників Волинського національного університету імені Лесі Українки (від 10 лютого 2017 р.) (<https://bit.ly/31NJD7N>)

Конфліктні ситуації вирішуються згідно Положення про порядок і процедури вирішення конфліктних ситуацій у Волинському національному університеті імені Лесі Українки (<https://bit.ly/33MTIM>).

Згідно Положення про академічну мобільність студентів (<https://bit.ly/3oMzMkk>), власне право неформальну освіту, здобувач може отримати додаткові бали, якщо бере участь у тренінгу, конференції, науковому семінарі, проблемній групі та ін.

Здобувач вчасно здає усі види робіт. Викладач інформує про терміни здачі лабораторних та контрольних робіт.

Здобувач має можливість скласти іспит згідно розкладу заліково-екзаменаційної сесії, має право скласти іспит повторно, а також скласти іспит комісії, у яку входять представники кафедри та деканату. Якщо за ці три можливості іспит не складено, здобувач виключається зі складу студентів Волинського національного університету імені Лесі Українки. В університетських положеннях є право на поновлення і проходження повторного проходження

Шкала оцінювання (національна та ECTS)

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсової роботи (проекту), практики	для заліку
90 – 100	A	Відмінно	Зараховано
82 – 89	B	Добре	
75 - 81	C		
67 -74	D	Задовільно	
60 - 66	E		
1 – 59	Fx	Незадовільно	Незараховано (з можливістю повторного складання)

РЕКОМЕНДОВАНІ ДЖЕРЕЛА

1. Острей О.Р. Системи моніторингу загроз. Дистанційний курс. URL: <http://194.44.187.60/moodle/enrol/index.php?id=1001>
2. Системи моніторингу загроз. Блог старшого викладача кафедри комп'ютерних наук та кібербезпеки Острей Оксани Ростиславівни. URL: https://ostreyoxana.blogspot.com/p/blog-page_60.html
3. Острей О.Р. Особливості викладання міжгалузевої дисципліни “Системи моніторингу загроз” - Міжпредметні зв'язки природничо-математичних дисциплін в освітньому процесі матеріали Всеукр. наук.-практ. інтернет -конф. (10-12 березня 2021року) / укладачі Н.А Головіна, Г.П Кобель, О.С Мартинюк. - Луцьк : Вежа-Друк, с.156-С.38-42
4. Галіцин В. К. Концептуальні засади моніторингу / В. К. Галіцин, О. П. Суслов, Н. К. Самченко // Бізнес Інформ. - 2013. - № 9. - С. 330-335.
5. Галіцин В. К. Системи моніторингу: Монографія. — К: КНЕУ, 2000. — 231 с.
6. Галіцин В. К. Системи моніторингу : Навчальний посібник / В. К. Галіцин, О. П. Суслов, Н. К. Самченко. — К. : КНЕУ, 2015. — 408 с.
7. Г. В. Корнійчук Моніторинг у системі управління фінансовим потенціалом підприємства - Інвестиції: практика та досвід № 13/2018. URL: <https://bit.ly/2QXSIGA>
8. Кривов'язюк І. В. Місце контролінгу і моніторингу в процесах прийняття та реалізації інвестиційних рішень на підприємстві [Електронний ресурс] / І. В. Кривов'язюк, Л. В. Кривов'язюк, О. І. Кривов'язюк // Економічні науки. – 2013. – URL: http://www.economy.nayka.com.ua/pdf/4_2018/58.pdf.
9. Чекурін В.Ф., Острей О.Р., Острей С.В., Модель функціонування інформаційно-аналітичної системи багаторівневого моніторингу якості освіти Фізико-математичне моделювання та інформаційні технології. – Львів. - 2007. - №6. - С. 66-76. – URL: <https://drive.google.com/file/d/1P5HcWaysf0QIcG0r9pNp9JNSsrQBbgSd/view>
10. Острей О.Р. Діаграма класів UML як засіб моделювання інформаційної системи моніторингу якості освіти Інформаційні технології в освіті: Збірник наукових праць. Випуск 2. – Херсон: Видавництво ХДУ, 2008. – С. 85-89.
11. Моніторинг та оцінка результатів – URL: <http://multycourse.com.ua/ua/page/21/45#2>
12. Посібник з моніторингу та оцінювання програм регіонального розвитку / Лендшел М., Винницький Б., Ратейчак Ю., Санжаровський І. За ред. Санжаровського І., Полянського Ю. – К.: К.І.С., 2007. – 80 с. – URL: <https://bit.ly/3cTEKsF>
13. Юрчук Н.П. Система моніторингу в управлінні ІТ-проектами – URL: http://www.economy.nayka.com.ua/pdf/4_2018/58.pdf
14. Ситник Г.П. Концептуальні засади забезпечення національної безпеки України : навч. посіб. : у 3 ч. / Г.П. Ситник, В.І. Абрамов, Д.Я. Кучма. - Ч. 1 : Філософсько-методологічні та системні основи забезпечення національної безпеки. - К. : НАДУ, 2009. - URL: <https://bit.ly/3cTEPwt>
15. Ситник Г.П. Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади): Підручник К.: НАДУ, 2011.–с. - URL:

http://library.iducz.dsns.gov.ua/weblib/books/magistratura/Sitnik_DU%20.pdf

16. Національна безпека України: теорія і практика. – URL: <https://scholar.google.com.ua/scholar?oi=bibs&hl=uk&cites=6011641028132937566>

17. Ілляшенко В.В. Теоретичні та нормативно-правові основи національної безпеки України - Перспективи розвитку сучасної науки - м. Львів, 5-6 грудня 2014р. - С. 127-129. – URL: <https://molodyvcheny.in.ua/files/conf/other/03dec2014/42.pdf>

18. Глобальна та національна безпека: підручник /авт. кол. :В.І. Абрамов, Г.П. Ситник, В.Ф. Смолянюк та ін. / за заг. ред. Г.П.Ситника. –Київ : НАДУ, 2016. –784с.– URL: <https://www.minregion.gov.ua/wp-content/uploads/2017/11/Navchalnyi-posibnik-GPNB.pdf>

19. Ситник Г. П. Національна безпека України: теорія і практика : монографія / Г. П. Ситник, В. М. Олуйко, М. П. Вавринчук ; за заг. ред. Г.П. Ситника. – Київ : Вид-во «Кондор», 2007. – 669 с.– URL: <http://elar.khnu.km.ua/jspui/handle/123456789/8690>

20. Антонов В. О.А 72 Конституційно-правові засади національної безпеки України: монографія / В. О. Антонов; наук. ред. Ю.С. Шемшученко. Київ: ТАЛКОМ, 2017. 576 с.– URL: <https://bit.ly/3dCpcIP>

21. Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку : збірник наукових праць за матеріалами її міжнародної науково-практичної конференції (8 червня 2018 р., м. Острого) / [за заг. ред. д.ю.н. романова м. с.]. – Острого: Видавництво Національного університету «Острозька академія», 2018. – 326 с. – URL: <https://bit.ly/3sRWREz>

22. Внукова Н. Н. Основи фінансового моніторингу фінансових послуг / Н. Н. Внукова. – К.: КНТ, 2009. – 136 с.

23. Система моніторингу поширення епідемії коронавірусу – URL: <https://covid19.rnbo.gov.ua/>

24. Системи моніторингу ІТ-інфраструктури – URL: <https://bit.ly/3wlptZf>

25. Системи моніторингу та управління безпекою – URL: <http://integritysys.com.ua/security/siem/>

26. Щодо впровадження системи моніторингу оцінювання результатів службової діяльності державних службовців, які займають посади категорії «Б» і «В» у міністерстві, іншому центральному органі виконавчої влади. – URL: <https://bit.ly/39HTqJg>

27. Системи моніторингу стану SIPLUS CMS – URL: <https://sie.ag/2Pz2IQT>

28. Системи моніторингу стану SKF – URL: <https://bit.ly/3sS6SBE>

29. В. В. Кулаженко, Система моніторингу економічної безпеки підприємства як чинник формування його конкурентоспроможності ефективна економіка № 8, 2016 – URL: <https://bit.ly/31Mkq60>

30. Варенко В.М.Інформаційно-аналітична діяльність: Навч. посіб. / В.М. Варенко. –К.: Університет «Україна», 2014. – 417с. – URL: <https://bit.ly/39GPZ5n>

31. Леонов С.В., Куришко О.О. Побудова системи внутрішнього фінансового моніторингу в фінансово-кредитних установах небанківського типу № 4 (25) 2011 бізнес-навігатор науково-виробничий журнал. – URL: <https://bit.ly/3wtJ3mb>

32. Захист інформації в комп'ютерних системах та мережах:навч. посіб./С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко –Х.: НТУ «ХПІ», 2014.–251с.– URL: <https://bit.ly/3wqB1KK>

33. Лабораторний практикум знавчальної дисципліни "Інформаційна безпека".

Навчально-практичний посібник/ С. В. Кавун,В. В. Носов, В. В.Огурцов, О. В.Манжай.

–Харків: Вид. ХНЕУ, 2008. –256с. (Укр. мов.) – URL: <https://bit.ly/39EjeGg>

34. Плікус І. Й. Система моніторингу для фінансового прогнозу діяльності підприємства / І. Й. Плікус // Фінанси України.– 2003.– № 4.– С. 35 – 44.

35. Шевяков А. Ю. Социально-экономический мониторинг: концепция, проблемы, перспективы / А. Ю. Шевяков, Г. Б. Клейнер // Экономика и математические методы. – 1993. – Т. 29. – Вып. 1. – С. 5 – 14

36. Прокопьев О. А. Сравнительный анализ организационных форм систем мониторинга реализации проектов / О. А. Прокопьев. // Вестник экономики, права и социологии. – 2012. – №2. – С. 68–72.

37. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. – К.:Інтертехнологія, 2009. – 164 с.

38. Матов О.Я., Василенко В.С., Будько М.М. Оцінка захищеності в локальних обчислювальних мережах // Вісті Академії інженерних наук України. — К., 2005. — № 2. — С. 59–73.

39. Приходько В. М. Парадигми моніторингу якості освіти і педагогічного процесу (у запитаннях і відповідях) / В. М. Приходько. – Х. : Вид. група «Основа», 2010. – 192 с.

40. Кириленко Н.М. Інформаційна безпека. Навчально-методичний посібник. – Вінниця: – ГЛОБУС-ПРЕС, 2017. – 416 с.

41. Біляєв С. С. Проектний підхід у підприємстві: сутність і специфічні ознаки / С. С. Біляєв // Держава та регіони. Серія : Економіка та підприємництво. – 2016. – № 3. – С. 30-34.

42. Ярошук Л. Г. Основи педагогічних вимірювань та моніторингу якості освіти: навчальний посібник / Л. Г. Ярошук – Бердянськ : Видавець Ткачук О. В., 2010. – 248 с.

43. Гошовська В.А. Соціальна домінанта національної безпеки // Стратегічна панорама. – 2003. – № 2. – С. 94-99.
44. Стратегія національної безпеки України в контексті досвіду світової спільноти // Зб. ст. за матеріалами міжнародної конференції. – Київ: САТСАНГА, 2001. – 224 с.
45. Стан техногенної та природної безпеки в Україні в 2015 році. Звіт МНС та НАН. [Електрон/ресурс]. – Режим доступу: http://www.mns.gov.ua/content/national_lecture.html.
46. Ситуаційні центри. Теорія і практика. НАН України. – ППММС. – К., 2009. – 347 с.
47. Гречанінов В.Ф. Інформаційні технології аналізу стану техногенної безпеки та планування протидії надзвичайним ситуаціям: автореф. дис. на здобуття наукового ступеня кандидата техн. наук: 05.13.06 / В.Ф. Гречанінов. – К., 2014. – 22 с.
48. Гречанінов В.Ф. Функції управління і нагляду в ризик-орієнтованому підході до управління безпекою / В.Ф. Гречанінов, В.В. Бегун // Математичні машини і системи. – К.: ППММС, 2014. – №1. – С. 159-170.
49. РД 211.0.8.107-05 Методичні рекомендації з питань створення систем моніторингу довкілля регіонального рівня, затверджені наказом Міністерства охорони навколишнього природного середовища України від 16.12.2005 N 467.
50. Інструкція щодо вимог пожежної безпеки під час проектування автозаправних станцій. Затверджено Наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи 06.12.2005 N 376.
51. Бегун В.В. Решение задачи определения текущего уровня риска (мониторинга) с применением алгоритмов МГУА / В.В. Бегун, В.В. Литвинов Моделирование 2012. ППМЕ ім. Г.Е. Пухова. – К., 2012. – С. 92-97.
52. Голуб С.В. Методологія створення автоматизованих систем багаторівневого соціоекологічного моніторингу: автореф. дис. на здобуття наук. ступеня д-ра техн. наук: 05.13.06 / С.В. Голуб. – К., 2008. – 35 с.
53. Актуальні проблеми моделювання ризиків і загроз критичних інфраструктур / В.Ф. Гречанінов, В.В. Бегун, В.П. Клименко, О.П. Яцук // Науковий вісник Укр.НДПБ. – 2015. – №1(31). – С. 125-134.