КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ
КАФЕДРА МАТЕМАТИЧНОЇ ІНФОРМАТИКИ

«ЗАТВЕРДЖУЮ»
Заступник декана з навчальної роботи
_____ Олена КАШПУР
«7» 05 2021 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

для студентів

галузь знань	**12 «Інформаційні технології»**
спеціальність	**122 «Комп'ютерні науки»**
освітній рівень	**магістр**
освітня програма	**«Бізнес інформатика»**
вид дисципліни	**обов'язкова**

Форма навчання	**денна**
Навчальний рік	**2021/2022**
Семестр	1
Кількість кредитів ECTS	6
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**залік**

Викладач: д.т.н., професор Володимир ЗАСЛАВСЬКИЙ (лекції, лабораторні заняття)

Пролонговано на 20 /20 н.р._____(_____) «___» 20___ р.
на 20 /20 н.р._____(_____) «___» 20___ р.

КИЇВ – 2021

Розробник:
Заславський Володимир Анатолійович, д.т.н., професор, професор кафедри математичної інформатики

«ЗАТВЕРДЖЕНО»
Зав. кафедри математичноої інформатики
_____ Василь ТЕРЕЩЕНКО
Протокол № 10 від « 27 » 04 2021 р.

Схвалено Гарантом освітньо-наукової програми «Бізнес інформатика»
_____Володимир ЗАСЛАВСЬКИЙ
« 6 » 05 2021 року

Схвалено науково-методичною комісією факультету комп'ютерних наук та кібернетики
Протокол від " 6 " травня 2021 року № 10
Голова науково-методичної комісії _____Людмила ОМЕЛЬЧУК
(підпис)
« 6 » травня 2021 року

1. Мета дисципліни.

Метою навчальної дисципліни “Безпека систем критичної інфраструктури”, як складового освітнього модуля ОНП «Бізнес інформатика», є формування у студентів магістрів теоретичних та практичних знань, методології та принципів дослідження, проектування, підтримки функціонування та науково-технічного супроводження критичних об’єктів та критичних інфраструктур. Отримання практичних навичок по системному аналізу криичних систем, формалізації математичних моделей та алгоритмів прийняття рішень, які використовуються при дослідженні безпеки критичних систем та інфраструктур.

2. Попередні вимоги до опанування або вибору навчальної дисципліни (*за наявності*):
Для успішного вивчення дисципліни “Безпека систем критичної інфраструктури” рівень освіти здобувача повинен відповідати наступним вимогам:

знати: методологію системного аналізу, математичні моделі, методи та алгоритми прийняття рішень, які використовуються при розробці та дослідженні складних технічних, еколого – економічних та організаційних систем;. основи розробки інформаційно-аналітичних систем, баз даних.

вміти: проводити формулювання та аналіз прикладних задач, визначати складність та підходи до їх розвязання, їх реалізізації як комплекс програм; вміти разом із однодумцями обговорювати проблемні ситуації та способи знаходження рішень; володіти навичками математичного моделювання з використанням ІТ технологій.

3. Анотація навчальної дисципліни:

Навчальна дисципліна “Безпека систем критичної інфраструкури”є обов’язковою дисципліною ОНП «Бізнес інформатика» за освітнім другим (магістерським) рівнем вищої освіти, галузі знань 12 «Інформаційні технології» спеціальності 122 «Комп'ютерні науки».

Викладається у 1 семестрі в **обсязі – 180 год.**

(6 кредитів ECTS*)* зокрема: *лекції – 32 год., лабораторні- 24 год., консультації – 4 год., самостійна робота – 120 год..* Завершується дисципліна – **заліком.**

В результаті вивчення навчальної дисципліни студенти повинні:

знати: законодавчу базу, що повязана із дослідженням об’єктів критичної інфраструкури; яким чином застосовується системна методологія та принцип різнотипності при забезпеченні безпеки критичних інфраструктур; математичні моделі та алгоритми оптимізації надійності та ефективності функціонування критичних систем на стадіях їх життєвого циклу; формуванні систем захисту (антитероризм).

вміти: знаходити проблемні задачі при дослідженні обєктів критичної інфраструктури, розробляти математичні моделі та алгоритми, які реалізують бізнес-процеси на етапах життєвого циклу, розробляти багатоверсійні проблемно-орієнтовані інтерфейси та створювати пілотні розробки програмних комплексів.

Навчальна дисципліна “Безпека систем критичної інфраструкури”є обов’язковою дисципліною професійної підготовки фахівців другого (магістерського рівня) рівня вищої освіти в рамках освітньо-наукової програми «Бізнес інформатика» та безпосередньо пов’язана із дисциплінами: «Інформаційні системи та технології», “Інноваційні технології: принцип різнотипності: теорія та практика».

4. Завдання (навчальні цілі): набуття знань, умінь та навичок (компетенцій) на рівні новітніх досягнень у дослідженні об’єктів критичної інфраструктури та розробці моделей,

алгоритмів та программного забезпечення для їх розробки та супроводження на стадіях життевого циклу, відповідно до освітньої кваліфікації «Магістр з комп'ютерних наук». Зокрема, розвивати:

ЗК1. Здатність до абстрактного системного мислення, розуміння принципів аналізу та синтезу.

ЗК2. Здатність застосовувати знання у практичних ситуаціях, які пов'язані із інформаційними технологіями, складними системами та бізнес процесами.

ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК5. Здатність спілкуватися іноземною мовою та працювати в міжнародному контексті.

ЗК6. Здатність вчитися й оволодівати сучасними знаннями, генерувати нові ідеї та інноваційні рішення (креативність).

ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК8. Здатність до міждисциплінарних досліджень.

ЗК11. Здатність розробляти й керувати проектами та бізнес процесами.

ЗК12. Здатність приймати обґрунтовані рішення.

ЗК13. Здатність оцінювати та забезпечувати якість виконуваних робіт.

ЗК14. Визначеність і наполегливість щодо поставлених завдань і взятих обов'язків.

ЗК15. Здатність діяти на основі етичних міркувань.

ФК1. Здатність до ідентифікації та аналізу проблем, формування варіантів рішень та їх оцінки, оцінки ризиків та їх наслідків при прийнятті управлінських рішень в різних галузях, опанування теоретичних і прикладних аспектів систем прийняття рішень та інформаційно-аналітичних систем.

ФК3. Здатність до дослідження та аналізу надвеликих масивів даних із складною структурою для прийняття обґрунтованих і зважених бізнес-рішень.

ФК4. Здатність застосовувати математичні моделі та методи, засоби організації масивів даних для розробки та аналізу складних систем та критичних інфраструктур, консолідації ресурсів, зберігання, дослідження та захисту інформації, розв'язання завдань моделювання та прогнозування стратегічних напрямків розвитку бізнесу, бізнес процесів та інновацій.

ФК8. Здатність використовувати сучасні ІКТ для розв'язання міждисциплінарних задач, розвивати й реалізовувати нові конкурентоздатні ідеї в галузі інформаційних технологій.

ФК9. Здатність враховувати соціальні і етичні аспекти професійної діяльності та спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).

ФК10. Творчість у застосуванні знань, здатність критично переосмислювати наявні інформаційні технології та відстежувати тенденції їх розвитку, що необхідно при реалізації бізнес процесів.

5. Результати навчання за дисципліною: *(описуються з детальною достовірністю для розробки заходів оцінювання)*

Результат навчання (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)	**Форми (та/або методи і технології)**	**Методи оцінювання та**	**Відсоток у підсумкові**

Код	Результат навчання	викладання і навчання	пороговий критерій оцінювання (за необхідності)	й оцінці з дисципліни
РН1.1	*Знати основи законодавчої бази, термінологію та поняття критичного елемента, критичного об'єкта, критичної інфраструктури та їх вплив на функціонування, життєдіяльність та безпеку.*	*Лекція, лабораторна робота, самостійна робота*	*Поточне оцінювання, лабораторні роботи 1, 2*	*10%*
РН1.2	*Знати сутність принципів ситемного аналізу та принтципу різнотипності (різноманіття) при їх застовсуванні для дослідження та супроводження критичних обєктиів на стадіях та етапах їх життєвого циклу.*	*Лекція, лабораторна робота, самостійна робота*	*Поточне оцінювання, лабораторні роботи 2, 3, 4*	*15%*
РН2.1	*Вміти застосовувати системну методологію при аналізі та формалізації математичних моделей, розробки алгориттмічного забезпечення для прийняття високовідповідальних рішень при дослідженні та забезпеченні ефективного функціонування критичних об'єктів та критичних інфраструктур.*	*Лекція, лабораторна робота, самостійна робота*	*Поточне оцінювання, лабораторні роботи 1, 3*	*15%*
РН3.1.	*Обгрунтувати рішення і приймати їх на основі реальних данних, що формуються при науково-технічному супроводженні критичних систем; спілкуватися із експертами, які розуміють проблеми проектування та функціонування систем на стадіях життєвого циклу, готувати звіти та робити презентиції*	*Лекція, лабораторна робота, самостійна робота*	*Поточне оцінювання, лабораторні роботи 1, 3, 4*	*30%*
РН4.1	*Відповідально ставитись до кожного кроку робіт, змін та модифікацй програмного забезпечення та структури об'єктів, нести відповідальність за їх якість, оскільки наслідки від реалізації небажаних подій та ризики мають значні негативні наслідки.*	*Лекція, лабораторна робота, самостійна робота*	*Поточне оцінювання, лабораторні роботи 1, 2, 3, 4*	*30%*

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання *(необов'язково для вибіркових дисциплін які не входять до блоків спеціалізації)*

Результати навчання дисципліни **Програмні результати навчання**	**РН 1.1**	**РН 1.2**	**РН 2.1**	**РН 3.1**	**РН 4.1**
(з опису освітньої програми)					
ПРН1. Ідентифікувати проблемні ситуації, виконувати їх дослідження на основі системного підходу та його принципів, здійснювати обґрунтований вибір методів та моделей для формування ефективних управлінських рішень, застосовувати моделі і методи прийняття рішень при дослідженні бізнес процесів в організаціях,	+	+	+	+	+

при прогнозуванні розвитку підприємств та в предметній області комп'ютерних наук.					
ПРН2. Використовувати моделі та методи прийняття рішень на основі теорії нечітких множин та в умовах невизначеності і ризиків в процесі управлінської діяльності, формулюванні нових інноваційних задач та підходів при реалізації бізнес-процесів в різних прикладних галузях.		+	+	+	
ПРН3. Опанувати нові інструменти роботи з даними, здійснюючи пошук та обробку інформації в мережах для прогнозування бізнес-процесів та ситуаційного управління, SWOP-аналізу, відгуків, розробки інформаційно-аналітичних систем для реалізації бізнес процесів в техніці, економічних та соціальних системах, сфері електронної комерції, медіа, соціальних мережах, банкингу, рекламній діяльності, охороні здоров'я, тощо.		+	+	+	
ПРН4. Вміти формулювати задачі моніторингу при дослідженні систем та аналізувати і ефективно використовувати великі об'єми даних різної природи, проектувати сховища даних, для видобутку нових даних і знань, здійснювати їх візуалізацію, використовувати їх при дослідженні бізнес-процесів та прийнятті відповідальних рішень, будувати і оцінювати регресивні моделі, що генеруються на основі цих даних.		+	+	+	+
ПРН5. Вміти аналізувати, оцінювати та обчислювати ризики з урахуванням корпоративних цінностей та системних інтересів, розробляти план управління ризиками для визначення необхідних профілактичних заходів, застосовувати дії для пом'якшення наслідків ризиків та непередбачених подій з метою мінімізації втрат.	+	+	+	+	+
ПРН9. Оцінювати, класифікувати, обґрунтовувати та формувати вимоги до інформаційно-аналітичних систем, що створюються та впроваджуються, використовуючи різні методи та технології.	+	+	+	+	+
ПРН11. Демонструвати результати виконаної роботи, створювати презентації, писати звіти та публікації за результатами виконаної роботи.		+		+	+
ПРН12. Розуміти, цілеспрямовано шукати, аналізувати і вибирати в інформаційно-довідникових та науково-технічних ресурсах і джерелах необхідні для рішення професійних і наукових задач сучасні досягнення науки і техніки з огляду на ціннісні орієнтири сучасного суспільства.	+	+	+	+	+

7. Схема формування оцінки.

7.1 Форми оцінювання студентів

- семестрове оцінювання:

1. Лабораторна робота 1. : РН 1.1, РН 2.1, РН 3.1, РН 4.1 – **20 балів/12 балів**.
2. Лабораторна робота 2. : РН 1.1, РН 1.2, РН 4.1 – **20 балів/12 балів**.
3. Лабораторна робота 3. : РН 1.2, РН 3.1, РН2.1, РН 4.1 – **20 балів/12 балів**
4. Лабораторна робота 4. : РН 1.2, РН 3.1, РН 4.1 – **20 балів/12 балів**
5. Поточне опитування: РН 1.1, РН 1.2, РН, РН 2.1, РН 3.1, РН 4.1–**20 балів/12 балів**

- підсумкове оцінювання (диференційований залік)*:*

Залік виставляється за результатами роботи студента впродовж усього семестру і не передбачає додаткових заходів оцінювання для успішних студентів.

Перелік питань на поточне оцінювання

1. Визначення поняття критичних систем (КС) та критичних інфраструктур (КІ).
2. Законодавчі засади для розуміння проблем критичних систем та критичних інфраструктур
3. Ідентифікація об’єктів КІ.
4. Типи та приклади КС та КІ.
5. Системный анализ об’єктів КІ, принципи системного аналізу при дослідженні КІ.
6. Особливості життєвого циклу КС та КІ. Проблеми мінімізації ризику на стадіях та етапах життєвого циклу КІ.
7. Важливість, значимість та критичність елементів КС та КІ.
8. Особливості дослідження та складові життевого циклу на стадії проектування КС та КІ.
9. Математичні моделі та методи забезпечення надійності та ефективності функціонування КС та КІ.
10. Математичні моделі та методи оптимального резервування елементів та складових модулів КС та КІ.
11. Проблеми планування технічного обслуговування КС та КІ в умовах обмежених ресурсів.
12. Старіння КС та КІ. Системний підхід та математичні моделі і алгоритми при виявленні, ранжуванні та усуненні дефектів в КС та КІ.
13. Задачі оптимізації формування комплексів методів виявлення дефектів в КС та КІ на основі використання різнотипних методів неруйнівного контролю.
14. Методична та інформаційно-аналітична підтримка науково-технічногое супроводження об’єктів КІ
15. Фізичний захист обєктів КІ. Антитерроризм.
16. Інформаційна безпека КС та КІ
17. Надзвичайні ситуації та КС і КІ.
18. Приватно-державне партнерство та проблеми забезпечення функціонування КС та КІ.

Лабораторні роботи

Лабораторна робота 1. На основі законодавчої бази та наукових джерел розробити тлумачний словник термінів, що попязані із КС та КІ.

Лабораторна робота 2. Розробити та реалізувати задачу оптимального розташування сервісних / екстрених служб для забезпечення безпеки КС та КІ.
Лабораторна робота 3. Розробити, формалізувати та реалізувати задачу розподілу ресурсів для активного захисту об'єктів критичної інфраструктури.
Лабораторна робота 4. Оцінити загрозу для обраного об’єкта критичної інфраструктури.

7.2 Організація оцінювання: *(обов’язково зазначається порядок організації передбачених робочою навчальною програмою форм оцінювання із зазначенням орієнтовного графіку оцінювання).*

Терміни проведення форм оцінювання:

1. Лабораторна робота 1: до 4 тижня семестру.
2. Лабораторна робота 1: до 7 тижня семестру.
3. Лабораторна робота 1: до 10 тижня семестру.
4. Лабораторна робота 1: до 14 тижня семестру.

За відсутності студента з поважних причин має право здавати лабораторні роботи протягом навчального семестру.

7.3 Шкала відповідності оцінок

Відмінно / Excellent	90-100
Добре / Good	75-89
Задовільно / Satisfactory	60-74
Незадовільно / Fail	0-59
Зараховано / Passed	60-100
Не зараховано / Fail	0-59

8. Структура навчальної дисципліни. Тематичний план лекцій і семінарських / практичних / лабораторних *(вибрати необхідне)* занять

№ п/п	Назва теми	Кількість годин		
		Лекції	Лабораторні	Самостійна робота
Частина 1.Поняття критичних систем та інфраструктури				
1	**Вступ**. **Тема 1.** *Поняття критичних систем (КС) та критичних інфраструктур (КІ), їх визначення та приклади, типи та характеристики критичних об’єктів. Законодавчі положення про безпеку обєктів КІ та КС.* *Самостійна робота: опрацювання лекційного матеріалу. Виконання лабораторних робіт.*	2	2	8

2	**Тема 2.** *Ідентифікація об'єктів КІ. Принципи системного аналізу при дослідженні об'єктів КІ. Самостійна робота: опрацювання лекційного матеріалу. Виконання лабораторних робіт.*	2		6
3	**Тема 3.** *Стадії та етапи життєвого циклу КС та КІ та його особливості. Проблеми подовження ресурсу функціонування КС. Самостійна робота: опрацювання лекційного матеріалу. Виконання лабораторних робіт.*	2	0	8
4	**Тема 4.** *Важливість, значимість та критичність елементів КС та об'єктів КІ. Оцінка критичності елементів та складових КІ. Самостійна робота: опрацювання лекційного матеріалу. Виконання лабораторних робіт.*	2	2	8
5	**Тема 5.** *Особливості процесів проектування КС та КІ із врахуванням сучасної елементої бази, числа складових компонент, вимог по термінах безвідмовного функціонування. Самостійна робота: опрацювання лекційного матеріалу. Виконання лабораторних робіт.*	2	2	8
Частина 2. Математичні моделі та алгоритми при дослідженні критичних систем				
6	**Тема 6.** *Математичні моделі та методи забезпечення високої надійності та ефективносьі КС. Структурна та функціональна надлишковість, врахування багатьох критеріїв та обмежень, багатофункціональність складових вузлів об'єктів. Самостійна робота: опрацювання лекційного матеріалу. Виконання лабораторних робіт.*	4	2	8
7	**Тема 7.** *Математичні моделі та алгоритми планування організації технічного обслуговування критичних обєктів (морські платформи по видобутку нафти та газу, АЕС, центри керування польотами, складові платіжних систем (банкомати). Самостійна робота: опрацювання лекційного матеріалу. Виконання лабораторних робіт.*	2	2	8
8	**Тема 8.** *Проблеми старіння критичних обєктів, пошук елементів що відмовили та ланцюгів відмов, формування технології заміни елементів. Організація експертних процедур виявлення та ранжування дефектів в критичних обєктах та електронних системах керування. Самостійна робота: опрацювання лекційного матеріалу. Виконання лабораторних робіт.*	2	2	6

9	***Тема 9.*** *Оптимізаційні моделі задач формування комплексів методів виявлення дефектів в КС та КІ на основі використання методів неруйнівного контролю, що побудовані на різних фізичних принципах.* *Самостійна робота: опрацювання лекційного матеріалу. Виконання лабораторних робіт.*	2	2	8
10	***Тема 10.*** *Типи дефектів (проектні, фізичні, дефекти взаємодії, відмова програмного забезпечення). Оцінка вагомості дефектів та їх вплив на функціонування складових та об'єкта в цілому.* *Самостійна робота: опрацювання лекційного матеріалу. Виконання лабораторних робіт.*	2	2	8
11	**Тема 11.** *Науково-технічне супроводження об'єктів КІ.* *Самостійна робота: опрацювання лекційного матеріалу. Виконання лабораторних робіт.*	2	0	8
12	***Тема 12.*** *Фізичний захист обєктів КІ, розподіл ресурсів для забезпечення ефективного захисту (математичні моделі та алгоритми).* *Самостійна робота: опрацювання лекційного матеріалу. Виконання лабораторних робіт.*	2	2	10
13	***Тема 13.*** *Боротьба з терроризм. Формування різнотипних систем захисту від терористичних дій на обєктах критичної інфраструктури. Транспортування небезпечних відходів.* *Самостійна робота: опрацювання лекційного матеріалу.*	2	2	10
14	***Тема 14.*** *Надзвичайні ситуації та безпека функціонування КС і КІ. Вплив пандемії коронавірусу на безпечне функіонуванння критичних систем.* *Самостійна робота: опрацювання лекційного матеріалу.*	2	0	8
15	***Тема 15.*** *Координація зусиль по забезпеченні безпеки об'єктів КІ. Приватно-державне партнерство та проблеми забезпечення безвідмовного функціонування КС та КІ.* *Самостійна робота: опрацювання лекційного матеріалу. Виконання л*	2	2	8
	ВСЬОГО	**32**	**24**	**120**

Загальний обсяг ***180*** *год.,* в тому числі:
Лекцій **–** ***32*** *год.*
Лабораторні заняття - ***24*** *год.*

Консультації - ***4*** *год.*
Самостійна робота **-** ***120*** *год.*

9. Рекомендовані джерела

Основні:

1. Todor Tagarev, “Bulgaria: Protecting National Critical Infrastructures with the Contribution of the Ministry of Defense,” *The European Journal of Critical Services and Infrastructure Protection* 1, no. 1 (October 2013): 28-31. ISSN 2344 – 3790

2.Зелена книга з питань захисту критичної інфраструктури в Україні: зб. мат-лів. Міжнар. експерт. нарад/упоряд. Д.С.Бірюков, С.І.Кондратов; за заг.ред. О.М.Суходолі.-К.: НІСДб 2015.-176 с.

3. Хенли Дж., Кумамото Е. Надежность сложных систем и оценка риска, М.:Машиностроение,1985.

4. Волкович В.Л., Волошин А.Ф., Заславский В.А., Ушаков И.А. Модели и методы оптимизации надёжности сложных систем, Киев, 1993.-312 с.

6. Згуровський М.З., Панкратова Н.Д. Основи системного аналізу, Київ видавнича група BHV, 2007.-544 с.

7.Проектирование надежных спутников связи. /Под редакцией академика М.Ф. Решетнева. (Библиотечка “Космическая связь”). – Томск: МГП "РАСКО", 1993. – 221 с. (Афанасьев В.Г., Верхотуров В.И., Заславский В.А., Зеленцов В.А. и др.)

8. Заславський В.А. Принцип разнотипности и проблемы обеспечения надежности сложных систем с высокой ценой отказа // Радіоелектронні і комп’ютерні системи. Науково–технічний журнал, 2008, №6 (33), С.76-78.

9. Заславський В.А., Єрмоленко Р.В., Сахно Н.В. Програмне забезпечення для управління безпечною експлуатацією парогенераторів АЕС // Комп’ютерні засоби, мережі та системи. Інститут кібернетики ім. В.М.Глушкова НАНУ. - 2009, №8 - С.18-27.

10.Заславський В.А., Бірюков Д.С., Євгієнко В.В., Франчук О.В. Моделювання та оцінка сценаріїв загроз для об’єктів критичної інфраструктури// Наукові записки НаУКМА. Том 99: Комп’ютерні науки.- 2009.- С. 97-107.

11.Харченко В.С., Яковлев С.В., Горбачик О,С. та ін. Забезпечення функціональної безпеки критичних інформаційно–керуючих систем : монографія/ за ред. В.С.Харченка, С.В.Яковлева. Харків: Константа,2019.-272 с.

12.Zaslavsky V., Ievgienko V. Critical infrastructure protection policy and type-variety principle in decision making Proceeding Firs International Workshop Critical Infrastructure safety and Security (CriSS-DESSERT”11), 11-13 May, Kirovograd, Ukraine, Vol.2, 2011.

13.Zaslavsky V., Ievgiienko Y. Risk analyses and redundancy for protection of critical infrastructure Monographs of System Dependability// Editor J.Mazurkiewicz, J.Sugier, T.Walkowiak, W.Zamojski, Oficyna Widawnicza Politechniki Wroclawskiej, Wroclaw, Poland, 2010, P.161-173.

14.Zaslavskyi V., Pasichna M. (2019) System Approach Towards the Creation of Secure and Resilient Information Technologies in the Energy sector/ Information & Security, 2019, p.318-330.

Zaslavskiy V., Pasichna, M.: AHP-Based Comparative Analysis of Electricity Generating Portfolios for the Companies in EU and Ukraine: Criteria, Reliability, Safety. Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and

Knowledge Transfer, May 15-18, 2017, Kyiv, Ukraine. Доступно: http://ceur-ws.org/Vol-1844/

16.Заславський В.А. Системи зберігання енергії: аспекти безпеки і оптимізації / В.А. Заславський, М.В. Пасічна // Наукові записки НаУКМА. Комп'ютерні науки – К. 2018 – том 1 – 16 с.

17. Норкин В.И., Гайворонский А.А., Заславский В.А.., Кнопов П.С. Модели оптимального распределения ресурсов для защиты критической инфопаструктуры. Кибернетика и системный анализ,2018,том 54, №5, с.13-26.

Додаткові:

1. Proceeding of the first International Workshop Critical Infrastructure Safety and Security) CriSS-DESSERT 2011) Edited by V.Kharchenko, T.Tagarev. Kharkiv, National Aerospace University named after N.E.Zhukovsky "Khai", vol.1 and vol.2, 2011.
2. Горбулин В. Как победить Россию в войне будущего.-К.:Брайт Букс, 2020.-256 с.

3. Михалевич В.С., Волкович В.Л. Вычислительные методы исследования и проектирования сложных систем. М.:Наука, 1982.

4. Заславський В.А. Принцип разнотипности и проблемы обеспечения надежности сложных систем с высокой ценой отказа // Радіоелектронні і комп'ютерні системи. Науково–технічний журнал, 2008, №6 (33), С.76-78.

5.Заславський В.А., Стрижак Г.О. Моніторинг транзакцій у платіжній системі з використанням теорії нечітких множин // Наукові записки НаУКМА.-Сер. Комп'ютерні науки .- 2008.-Т.86.- С.35-39.

6.Безопасность критических інфраструктур:математические и инженерные методы анализа и обеспечения. Под ред. В.С.Харченко Проект ТЕМПУС SAFEGUARD, 2011.-641 с.