НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

факультет цивільного захисту

кафедра управління та організації діяльності у сфері цивільного захисту

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Прикладні інформаційні технології та кібербезпека
(назва навчальної дисципліни)

загальна обов'язкова
(обов'язкова загальна або обов'язкова професійна або вибіркова)

за освітньо-професійною програмою «Охорона праці»

підготовки ступеня магістра

у галузі знань 26 «Цивільна безпека»

за спеціальністю 263 «Цивільна безпека»

Рекомендовано кафедрою управління та організації діяльності у сфері цивільного захисту на 2022-2023 навчальний рік.
Протокол від «22» серпня 2022 року № _1___

Силабус розроблений відповідно до Робочої програми навчальної дисципліни «Прикладні інформаційні технології та кібербезпека»

2022 рік

Загальна інформація про дисципліну

Анотація дисципліни

Знання отримані під час вивчення навчальної дисципліни «Прикладні інформаційні технології та кібербезпека» спрямовані на формування у здобувачів вищої освіти необхідного в їх подальшій професійній діяльності рівня знань та умінь з питань використання інформаційних технологій для розв'язання складних завдань у сфері цивільної безпеки, критерії оцінки їх захищеності і методи забезпечення їх інформаційної безпеки.

Інформація про науково-педагогічного працівника

Загальна інформація	Лєвтєров Олександр Антонович, доцент кафедри управління та організації діяльності у сфері цивільного захисту факультету цивільного захисту, доктор технічних наук, старший науковий співробітник
Контактна інформація	м. Харків, вул. Баварська, 7, кабінет №114.
E-mail	levterov@nuczu.edu.ua
Наукові інтереси*	Моделювання у сфері цивільного захисту; інформаційні технології та захист інформації у сфері цивільного захисту; Системний аналіз.
Професійні здібності*	Навички: аналізу науково-технічної, довідникової, нормативної та патентної літератури; навички аналітичних розрахунків та моделювання досліджень, пов'язаних з раннім виявленням пожежі; експериментальних досліджень; проектування та побудови випробувальних стендів, експериментальних діючих зразків, комплексів засобів вимірювальної техніки. Професійні знання і значний досвід роботи в Android SDK, SQLite, Rad Studio, C++, C. DD, Adobe Audition, Matlab
Наукова діяльність за освітнім компонентом	Розробка акустичного методу для раннього виявлення джерел загорань. Розробка шляхів удосконалення моніторингу та прогнозування сейсмічної небезпеки локальної території земної кулі. Дослідження шляхів удосконалення моніторингу надзвичайних ситуацій за допомогою безпілотних літальних апаратів. Формалізація процесу виникнення та ліквідації надзвичайних ситуацій на території областей україни. Розробка моделі прогнозування залучення оперативно-рятувальних підрозділів харківської області до ліквідації надзвичайних подій.

Час та місце проведення занять з дисципліни

Аудиторні заняття з навчальної дисципліни проводяться згідно затвердженого розкладу. Електронний варіант розкладу розміщується на сайті Університету (http://rozklad.nuczu.edu.ua/timeTable/group).

Консультації з навчальної дисципліни проводяться протягом семестру щочетверга з 16.00 до 17.00 в аудиторії № 901. В разі додаткової потреби здобувача в консультації час погоджується з викладачем.

Мета вивчення дисципліни: підготовка здобувачів вищої освіти, здатних розробляти програмне забезпечення за допомогою об’єктно-орієнтованої мови Java для розв’язання важливих прикладних задач у сфері цивільного захисту; оцінювати кібербезпеку у системі національної безпеки України передбачати загрози інформаційній безпеці держави, використовувати сучасні підходи до побудови систем захисту інформації та комп'ютерних систем.

Опис навчальної дисципліни

Найменування показників	Форма здобуття освіти
	заочна (дистанційна)
Статус дисципліни	обов’язкова професійна
Рік підготовки	1
Семестр	2
Обсяг дисципліни:	
- в кредитах ЄКТС	4
- кількість модулів	2
- загальна кількість годин	120
Розподіл часу за навчальним планом:	
- лекції (годин)	10
- практичні заняття (годин)	2
- семінарські заняття (годин)	–
- лабораторні заняття (годин)	–
- курсовий проект (робота) (годин)	–
- інші види занять (годин)	–
- самостійна робота (годин)	108
- індивідуальні завдання (науково-дослідне) (годин)	–
- підсумковий контроль (диференційний залік, екзамен)	екзамен

Передумови для вивчення дисципліни

Наявність освітнього ступеня бакалавра, вивчення навчальної дисципліни «Теорія систем та системного аналізу».

Результати навчання та компетентності з дисципліни

Відповідно до освітньої програми «Охорона праці» вивчення навчальної дисципліни повинно забезпечити:

- досягнення здобувачами вищої освіти таких результатів навчання

Програмні результати навчання	ПРН
Використовувати сучасні інформаційні та комунікаційні технології, спеціалізоване програмне забезпечення під час розв’язання практичних задач	ПРН 7
Відшуковувати необхідну інформацію в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об’єктивно оцінювати інформацію	ПРН 17
Дисциплінарні результати навчання	*абревіатура*
Використовувати сучасні підходи до побудови систем захисту інформації та комп'ютерних систем	ДРН 1
Використовувати інформаційні технології для розв’язання складних завдань у сфері цивільної безпеки	ДРН 2

- формування у здобувачів вищої освіти наступних компетентностей:

Програмні компетентності (загальні та професійні)	ЗК, ПК
Здатність до пошуку, оброблення та аналізу інформації з різних джерел	ЗК 1
Здатність приймати ефективні рішення, керувати роботою колективу під час професійної діяльності	ПК1
Здатність застосовувати сучасні інформаційні та комунікаційні технології, спеціалізоване програмне забезпечення у сфері професійної діяльності	ПК 6
Очікувані компетентності з дисципліни	*абревіатура*
Здатність розробляти програмне забезпечення за допомогою об’єктно-орієнтованої мови Java для розв’язання важливих прикладних задач у сфері цивільної безпеки	ДК 1
Здатність оцінювати кібербезпеку у системі національної безпеки України передбачати загрози інформаційній безпеці держави	ДК 2

Програма навчальної дисципліни

Теми навчальної дисципліни:

МОДУЛЬ 1. Основи об’єктно-орієнтованої мови програмування Java та розробка прикладних програм.

Тема 1.1. Загальні відомості про Java.

Тема 1.2. Типи даних та змінні у Java.

Тема 1.3. Приведення типів даних у Java. Масиви.

Тема 1.4. Операції в мові Java.

Тема 1.5. Управляючі оператори в Java.

Тема 1.6. Основи роботи з класами у Java.

МОДУЛЬ 2. Основи кібербезпеки та розробка рекомендацій по забезпеченню інформаційної безпеки

Тема 2.1. Предмет курсу. Інформаційна безпека та кібербезпека в системі національної безпеки України.

Тема 2.2. Основні поняття теорії інформаційної безпеки.

Тема 2.3. Аналіз загроз інформаційній безпеці.

Тема 2.4. Методи і засоби забезпечення інформаційної безпеки.

Тема 2.5. Основи комплексного забезпечення інформаційної безпеки. Моделі, стратегії (політики) і системи забезпечення інформаційної безпеки.

Тема 2.6. Стандарти інформаційної безпеки, критерії та класи оцінки захищеності комп'ютерних систем і мереж.

Тема 2.7. Методологія побудови та аналізу систем забезпечення інформаційної безпеки.

Розподіл дисципліни у годинах за формами організації освітнього процесу та видами навчальних занять:

Назви модулів і тем	**Заочна (дистанційна)**					
	Кількість годин					
	усього	у тому числі				
		лекції	практичні (семінарські) заняття	лабораторні заняття (інші види занять)	самостійна робота	модульна контрольна робота
2- й семестр						
Модуль 1. Основи об’єктно-орієнтованої мови програмування Java та розробка прикладних програм						
Тема 1.1. Загальні відомості про Java	8	2	–	–	6	–
Тема 1.2. Типи даних та змінні у Java	8	–	–	–	8	–
Тема 1.3. Приведення типів даних у Java.	8	–	–	–	8	–

Масиви						
Тема 1.4. Операції в мові Java	8	2	–	–	6	–
Тема 1.5. Управляючі оператори в Java	8	–	–	–	8	–
Тема 1.6. Основи роботи з класами у Java	20	2	–	–	18	–
Разом за модулем 1	60	6	–	–	54	–
Модуль 2. Основи кібербезпеки та розробка рекомендацій по забезпеченню інформаційної безпеки						
Тема 2.1. Предмет курсу. Інформаційна безпека та кібербезпека в системі національної безпеки України	8	–	–	–	8	–
Тема 2.2. Основні поняття теорії інформаційної безпеки	8	2	–	–	6	–
Тема 2.3. Аналіз загроз інформаційній безпеці	8	–	–	–	8	–
Тема 2.4. Методи і засоби забезпечення інформаційної безпеки	10	-	2	–	8	–
Тема 2.5. Основи комплексного забезпечення інформаційної безпеки. Моделі, стратегії. Системи забезпечення інформаційної безпеки	8	–	–	–	8	–
Тема 2.6. Стандарти інформаційної безпеки, критерії та класи оцінки захищеності комп'ютерних систем і мереж	10	2	-	–	8	–

Тема 2.7. Методологія побудови та аналізу систем забезпечення інформаційної безпеки	8	–	–	–	8	-
Разом за модулем 2	60	4	2	–	54	–
Разом	**120**	**10**	**2**	**–**	**108**	**–**

Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Методи і засоби забезпечення інформаційної безпеки	2

Орієнтована тематика індивідуальних завдань у вигляді: рефератів, тез доповідей, доповіді на конференції

1. Аналіз загроз інформаційній безпеці в Україні
2. Прикладне програмне забезпечення у сфері цивільної безпеки
3. Законодавство у сфери інформаційної безпеки в Україні
4. Основи комплексного забезпечення інформаційної безпеки та системи забезпечення інформаційної безпеки.
5. Об’єктно-орієнтоване програмування.

В навчальній дисципліні використовуються такі методи навчання і викладання:

МН1. Словесні методи навчання (спонукають здобувачів до створення в уяві певного образу, приведення попередніх знань до усвідомлення нових явищ та понять).

МН2. Практичні методи навчання (сприяють формуванню вмінь і навичок, логічному завершенню ланки пізнавального процесу стосовно конкретної теми або розділу).

МН3. Наочні методи навчання (передбачають демонстрацію, ілюстрацію та спостереження (сприймання процесів без втручання у ці процеси)).

МН4. Робота з навчально-методичною літературою та відеометод у сполучен-ні з новітніми інформаційними техно-логіями та комп'ютерними засобами навчання.

МН5. Самостійна робота (спрямована на використання набутих знань при розв’язанні програмних завдань)

Оцінювання освітніх досягнень здобувачів вищої освіти

Засоби оцінювання

Засобами оцінювання та методами демонстрування результатів навчання є: опитування на практичному занятті, виконання та захист

контрольної роботи, екзамен.

Оцінювання рівня освітніх досягнень здобувачів за освітніми компонентами, здійснюється за 100-бальною шкалою, що використовується в НУЦЗ України з переведенням в оцінку за рейтинговою шкалою – ЄКТС та в 4-бальну шкалу.

Таблиця відповідності результатів оцінювання знань з навчальної дисципліни за різними шкалами

За 100-бальною шкалою, що використовується в НУЦЗ України	За рейтинговою шкалою (ЄКТС)	За 4-бальною шкалою
90–100	A	відмінно
80–89	B	добре
65–79	C	
55–64	D	задовільно
50–54	E	
35–49	FX	незадовільно
0–34	F	

Критерії оцінювання

Форми поточного та підсумкового контролю

У процесі вивчення дисципліни здобувачі вищої освіти виконують контрольну роботу, яка охоплює 2 модулі.

Підсумковий контроль проводиться у формі екзамену.

Розподіл та накопичення балів, які отримують здобувачі, за видами навчальних занять та контрольними заходами з дисципліни

Види навчальних занять	Кількість навчальних занять	Максимальний бал за вид навчального заняття	Сумарна максимальна кількість балів за видами навчальних занять
І. Поточний контроль			
практичні заняття*	1	10	10
Виконання контрольної роботи*			40
Разом за поточний контроль			50
Індивідуальне дослідне завдання **			15
ІІ. Підсумковий контроль (екзамен)			50
Разом за всі види навчальних занять та контрольні заходи			100

** обов'язкове для виконання*

***не обов'язкове для виконання*

Форми поточного та підсумкового контролю

Поточний контроль проводиться у формі індивідуального опитування. У процесі вивчення дисципліни здобувачі вищої освіти виконують контрольну роботу.

Підсумковий контроль проводиться у формі екзамену.

Критерії поточного оцінювання знань здобувачів на практичному занятті:

10 балів – питання розкрито в повному обсязі, відповідь вірна, наведено аргументацію, використовуються професійні терміни, звіт о виконанні завдання оформлено грамотно та без помилок;

5-9 балів – питання розкрито, але обґрунтування відповіді недостатнє або звіт оформлено з помилками;

1-4 балів – питання розкрито, але обґрунтуване недостатньо та з помилками;

0 балів – завдання не виконане.

За виконання індивідуального завдання

15 балів – вірно розв’язано завдання з дотримуванням всіх вимог до виконання;

10 балів – вірно розв’язано завдання, але недостатнє обґрунтування відповіді, допущені незначні граматичні чи стилістичні помилки;

5 балів –надано відповідь на одне питання;

0 балів – відповідь відсутня.

Критерії оцінювання знань здобувачів під час виконання контрольної роботи:

40 балів – вірно розв’язано завдання з дотримуванням всіх вимог до виконання;

30-39 балів – вірно розв’язано завдання, але недостатнє обґрунтування відповіді, допущені незначні граматичні чи стилістичні помилки;

20-29 балів – розв’язано задачу та надано відповідь на одне питання;

10-19 балів – розв’язана одна задача;

1-9 балів – надано тільки відповіді на теоретичні питання;

0 балів – відповідь відсутня.

Питання для виконання контрольної роботи

1. Основні принципи об’єктно-орієнтованого програмування.
2. Цілочисельні типи даних у Java.
3. Типи даних з плаваючою точкою.
4. Символи та логічні значення у Java.
5. Оголошення змінної у Java. Динамічна ініціалізація.
6. Область та термін дії змінних.
7. Автоматичне перетворення типів у Java. Приведення несумісних типів.
8. Автоматичне просування типів у виразах. Правила просування типів.

9. Робота з масивами у Java.

10. Арифметичні операції. Арифметичні операції з присвоєнням.

11. Операції відношення та логічні операції.

12. Операції присвоєння. Тернарний оператор. Першочерговість операцій.

13. Умовний оператор if.

14. Оператор розгалуження switch.

15. Оператор циклу while.

16. Оператор циклу do-while.

17. Оператор циклу for.

18. Різновиди циклу for.

19. Оператори переходу.

20. Загальна форма класу.

21. Оголошення об’єктів.

22. Методи класів.

23. Конструктори класів.

24. Ключові слова this, static, final.

25. Перевантаження методів.

1. Законодавство України з інформаційної безпеки. Кібербезпека.

2. Роль інформаційної безпеки в забезпеченні національної безпеки держави.

3. Види безпеки особистості.

4. Види інформації, що захищається.

5. Основні поняття і загально принципи теорії інформаційної безпеки.

6. Забезпечення інформаційної безпеки в нормальних і надзвичайних ситуаціях.

7. Основні правові та нормативні акти у сфері інформаційної безпеки.

8. Основні поняття теорії комп'ютерної безпеки.

9. Суб'єктно-об'єктна модель інформаційної системи.

10. Цінність інформації. Аддитивна модель. Порядкова шкала. Решітка цінності.

11. Загрози конфіденційності, цілісності, доступності інформації, розкриття параметрів інформаційної системи.

12. Рівні захисту інформації.

13. Захист носіїв інформації.

14. Захист засобів взаємодії з носите лями інформації.

15. Захист подання інформації.

16. Захист змісту інформації.

17. Основні види атак на інформаційні системи.

18. Класифікація основних атак і шкідливих програм.

19. Організаційно режимні заходи. Захист від несанкціонованого доступу.

20. Побудова пральних систем.

21. Криптографічні методи захисту.

22. Основні методи захисту пам'яті.

23. Цифровий підпис.
24. Захист від збоїв програмно-апаратної середовища.
25. Приховування характеристик носіїв.
26. Поняття політики безпеки.
27. Моделі безпеки.
28. Застосування ієрархічного методу для побудови захищеної системи.

Підсумковий контроль.

Критерії оцінювання знань здобувачів на екзамені:

50 балів – в повному обсязі здобувач володіє навчальним матеріалом, глибоко та всебічно розкрив зміст усіх завдань з повним дотримуванням вимог до виконання;

38-49 балів – достатньо повно володіє навчальним матеріалом, в основному розкрито зміст завдань. При наданні відповіді на деякі питання не вистачає достатньої глибини та аргументації, при цьому є несуттєві неточності та незначні помилки;

26-37 балів – в цілому володіє навчальним матеріалом, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускає при цьому окремі суттєві

13-25 балів – не в повному обсязі володіє навчальним матеріалом. Недостатньо розкриті зміст завдань з допущенням при цьому суттєвих неточностей;

1-12 бал – частково володіє навчальним матеріалом, відповіді загальні, допущено при цьому суттєві помилки;

0 балів – не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту завдань.

Перелік теоретичних питань для підготовки до екзамену:

1. Основні принципи об’єктно-орієнтованого програмування.
2. Цілочисельні типи даних у Java.
3. Типи даних з плаваючою точкою.
4. Символи та логічні значення у Java.
5. Оголошення змінної у Java. Динамічна ініціалізація.
6. Область та термін дії змінних.
7. Автоматичне перетворення типів у Java. Приведення несумісних типів.
8. Автоматичне просування типів у виразах. Правила просування типів.
9. Робота з масивами у Java.
10. Арифметичні операції. Арифметичні операції з присвоєнням.
11. Операції відношення та логічні операції.
12. Операції присвоєння. Тернарний оператор. Першочерговість операцій.
13. Умовний оператор if.

14. Оператор розгалуження switch.
15. Оператор циклу while.
16. Оператор циклу do-while.
17. Оператор циклу for.
18. Різновиди циклу for.
19. Оператори переходу.
20. Загальна форма класу.
21. Оголошення об’єктів.
22. Методи класів.
23. Конструктори класів.
24. Ключові слова this, static, final.
25. Перевантаження методів.
26. Законодавство України з інформаційної безпеки. Кібербезпека.
27. Роль інформаційної безпеки в забезпеченні національної безпеки держави.
28. Види безпеки особистості.
29. Види інформації, що захищається.
30. Основні поняття і загально принципи теорії інформаційної безпеки.
31. Забезпечення інформаційної безпеки в нормальних і надзвичайних ситуаціях.
32. Основні правові та нормативні акти у сфері інформаційної безпеки.
33. Основні поняття теорії комп'ютерної безпеки.
34. Суб'єктно-об'єктна модель інформаційної системи.
35. Цінність інформації. Адитивна модель. Порядкова шкала. Решітка цінності.
36. Загрози конфіденційності, цілісності, доступності інформації, розкриття параметрів інформаційної системи.
37. Рівні захисту інформації.
38. Захист носіїв інформації.
39. Захист засобів взаємодії з носите лями інформації.
40. Захист подання інформації.
41. Захист змісту інформації.
42. Основні види атак на інформаційні системи.
43. Класифікація основних атак і шкідливих програм.
44. Організаційно режимні заходи. Захист від несанкціонованого доступу.
45. Побудова пральних систем.
46. Криптографічні методи захисту.
47. Основні методи захисту пам'яті.
48. Цифровий підпис.
49. Захист від збоїв програмно-апаратної середовища.
50. Приховування характеристик носіїв.
51. Поняття політики безпеки.
52. Моделі безпеки.
53. Застосування ієрархічного методу для побудови захищеної системи.

Політика викладання навчальної дисципліни:

– Ативна участь в обговоренні навчальних питань, попередня підготовка до практичних занять за рекомендованою літературою, якісне і своєчасне виконання завдань

– Сумлінне дотримання розкладу занять з навчальної дисципліни (здобувачі вищої освіти, які запізнилися на заняття, до заняття не допускаються).

– Під час заняття мобільними пристроями дозволяється користуватися тільки з навчальною метою і з дозволу керівника заняття.

– Дотримання здобувачами вищої освіти політики доброчесності під час виконання модульних контрольних робіт та під час підсумкового контролю;

– Виконання інших вимог, що не суперечать законодавству України та нормативним документам Університету.

– Здобувач вищої освіти має право дізнатися про свою кількість накопичених балів у викладача навчальної дисципліни та вести власний облік цих балів.

– Суворе дотримання правил безпеки під час організації виїзних занять на об'єкти (не) виробничої сфери.

– У разі несвоєчасного виконання та захисту звіту з практичної або лабораторної роботи, поставленого індивідуального завдання, порушення терміну захисту індивідуального завдання, ліквідації заборгованості щодо індивідуального завдання загальна оцінки знижується на 50 відсотків.

– Терміни захисту та виконання індивідуального наукового завдання встановлюються організаторами конференції, яка пропонується викладачем для вибору здобувачу вищої освіти протягом семестру.

– Ліквідація поточної заборгованості відбувається протягом семестру.

– Процент уникальності при виконанні індивідуальних робіт не менше 70 %.

– Здобувач допускається до складання підсумкового семестрового контролю, якщо він виконав усі види обов'язкових робіт, що передбачені відповідною робочою програмою навчальної дисципліни (іншими навчально-методичними матеріалами з освітнього компонента) в семестрі та набрав за них необхідну кількість балів для допуску до підсумкового семестрового контролю.

– Здобувач, який не з'явився на підсумковий семестровий контроль освітнього компонента без поважних причин, вважається таким, який не склав цей підсумковий семестровий контроль та не виконав свого індивідуального плану.

– Здобувачеві, який не склав підсумкового семестрового контролю, керівник факультету дозволяє повторне складання підсумкового контролю з освітнього компонента за окремим графіком на строк до двох тижнів від початку наступного весняного семестру або до початку наступного осіннього

семестру.

– Додаткове складання іспиту допускається не більше двох разів із навчальної дисципліни: перший раз науково-педагогічному працівникові, другий – комісії, яка створюється за поданням керівника факультету розпорядженням проректора з навчальної та методичної роботи.

– Підвищення оцінки за екзамену або диференційований залік із певної навчальної дисципліни, з дозволу керівника факультету, здобувачеві може бути надана така можливість повторного складання цього підсумкового контролю, який був складений в одному із минулих підсумкових семестрових контролів. Здобувачеві може бути надана можливість повторного складання екзамену або диференційованого заліку.

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Література

1. Mathematical Model of Management of the Integral Risk of Emergency Situation on the Example of Fires / [Kravtsiv S., Sobol O., Komyak V., Danilin O., Al'boschiy O.] // IFIP Advances in Information and Communication Technology, 2020, 575 IFIP, c. 182-195.
2. Kravtsiv S.Ya. Determination of the limits of the application of the statistical method for evaluation integral fire risks / S.Ya Kravtsiv, O.M. Sobol, T.Ya. Samiliv // Проблеми надзвичайних ситуацій. – Харків: НУЦЗУ, 2018. – Вип. 27. – С. 47-51.
3. Формування динамічної моделі оперативного моніторингу рівня забруднення екосистеми внаслідок аварій на об'єктах ядерної енергетики / [В.В. Тютюник, О.М. Соболь, В.Д. Калугін, Ю.В. Захарченко] // Екологічна безпека та природокористування. – Київ: КНУБА, ІТіГІП, 2020, №1(33). – С. 95-114.
4. Модель оперативного моніторингу рівня забруднення екосистеми за допомогою безпілотних літальних апаратів / [Соболь О.М., Захарченко Ю.В., Тютюник В.В., Калугін В.Д., Квасов В.А.] // Проблеми охорони навколишнього природного середовища та екологічної безпеки. – Харків: ХНУ імені В.Н. Каразіна, 2020. – Вип. 42. – С. 178-199.
5. Соболь О.М., Ященко О.А., Кравців С.Я. Розробка Android-додатку для визначення інтегральних ризиків небезпечних подій / Conference Proceedings of the International Scientific Online Conference Topical Issues of Society Development in the Turbulence Conditions (May 30, 2020, Bratislava, Slovak Republic). The School of Economics and Management in Public Administration in Bratislava, 2020; pp. 295-299.
6. Соболь О.М. автоматизація визначення ступеня ризику від провадження господарської діяльності за допомогою програмного забезпечення для мобільних пристроїв / Міжнародна науково-практична

конференція "Проблеми надзвичайних ситуацій" 20 травня 2020 р. – Харків: НУЦЗУ, 2020. – С. 245-247.

7. Improving living standards: current opportunities and limitations / Соболь О.М., Бордюженко С.Я., Ляшевська О.І. // Editors: Wojciech Duczmal, Iryna Ostopolets. Opole: The Academy of Management and Administration in Opole, 2020; ISBN 978-83-66567-21-4; pp.594.

8. Соболь О.М., Ляшевська О.І., Соболь І.П. постановка задачі побудови комп'ютерної моделі поля радіоактивного забруднення / Збірник тез доповідей Міжнародної науково-практичної конференції "Графічні технології моделювання об'єктів, процесів та явищ", 23-24 квітня 2020 р. – Одеса: Військова академія, 2020. – С. 107.

9. Моніторинг надзвичайних ситуацій. Підручник / [Абрамов Ю.О., Грінченко Є.М., Кірочкін О.Ю. та ін.]. – Харків: АЦЗУ, 2005. – 530 с.

10. Інформатика та інформаційні технології у цивільній безпеці: практикум / Л.В. Гусева, М.М. Журавський, М.В. Маляров та ін. – Харків: НУЦЗУ, 2015. – 322 с.

11. Тимчук, С. А. Применение БПЛА и систем дистанционного контроля и поиска повреждений ЛЭП на основе клиент-серверного приложения / С.А. Тимчук, А.А. Левтеров, Ю.А. Нечитайло // Инженерия природополь- зования, Харьков: ХНТУСХ. – 2020, No2 (16). – С. 6 – 11. https://doi.org/10.37700/enm.2020.2(16).6 – 11

12. Левтеров А.А., Грицына И.Н. К оптимальному размещению пунктов дистанционного мониторинга с применением эволюционных вычислений. Проблеми надзвичайних ситуацій. Збірка наукових праць. 2016. Вип. 23. С. 84-88. (Стаття у міжнародних наукометричних базах Ulrich's Periodicals Directory, Index Copernicus, Research Bib, Google Scholar)

13. Levterov A.A., Levterov A.M. Thermodynamic properties of fatty acid esters in some biodiesel fuels. Functional materials, НТК «Інститут монокристалів» НАН України. 2018. P. 308-312.

14. Лєвтєров О.А., Шевченко Р.І. Апаратно-програмна реалізація сучасних підходів з попередження надзвичайних ситуацій природного характеру. Проблеми надзвичайних ситуацій. 2019. № 1(29). С. 47-60.

15. Levterov A.A. Acoustic Research Method for Burning Flammable Substances. Acoustical Physics. Volume 65. 2019. №4. P. 444–449.

16. Левтеров А.А., Шевченко Р.И. Построение электронного комплекса по расчету и оптимальному выбору аварийных вентиляционных систем. Проблеми надзвичайних ситуацій. Сб. науч. тр. - Харьков: АЦЗУ. 2006. Вып. 3. С. 138-144.

17. Левтеров А.А., Шевченко Р.И. Анализ надежности прикладного программного обеспечения при проектировании автоматизированных систем пожарной безопасности. Проблемы пожарной безопасности. Сб. науч. тр. Харьков: АЦЗУ. 2006. Вып. 19. С. 183-192.

18. Левтеров А.А., Гринченко Е.Н., Шевченко Р.И. Анализ методики расчета газового пожаротушения (ДБН В. 2.5-13-98*). Проблемы пожарной безопасности. Сб. наук. тр. Харьков: УГЗУ 2008. Вип. 23. С. 61-68.

19. Левтеров А.А., Климчук Ю. Особливості застосування комп’ютерних технологій в підготовці спеціалістів органів дізнання державного пожежного нагляду МНС України. Новий колегіум. Х.: ПФ "Колегіум". 2010. № 6. С.51-55.

20. Левтеров А.А. Оценка информационной безопасности и надежности программных средств органов и подразделений ГСЧС. Проблеми надзвичайних ситуацій. Збірка наукових праць. 2015. Вип. 21. С. 46-51.

21. Левтеров А.А. Прогнозирование чрезвычайной ситуации природного характера с использованием генетических алгоритмов. Проблеми надзвичайних ситуацій. Збірка наукових праць. 2015. №22. С.84-92.

22. Левтеров А.А., Левтеров А.М., Левтерова Л.И. Формирование базы данных термодинамических свойств сложных эфиров жирных кислот биодизельных топлив в газовой фазе (часть 1). Вісник Національного технічного університету "ХПІ". Серія : Математичне моделювання в техніці та технологіях. 2016. № 6. С. 30-37.

23. Левтеров А.А., Нечитайло Ю.А., Лычман М.А. Расчет MEL-коэффициентов звукового спектра для модуля идентификации голосовых команд управления мобильным роботом. Технология приборостроения. 2017. № 2. С. 36-39.

24. В.А. Андронов, Ю.П. Ключка, О.А. Лєвтєров. Особливості розробки електронної бази даних пожежовибухонебезпечних речовин і матеріалів для підрозділів дснс україни. Системи обробки інформації, 2014, випуск 9 (125). С.209-211

Інформаційні ресурси

11. Java Technologies at Oracle [Електронний ресурс]. – Режим доступу: https://developer.oracle.com/java/.

12. IntelliJ IDEA [Електронний ресурс]. – Режим доступу: https://www.jetbrains.com/idea/.

Розробник:

доцент кафедри управління та організації діяльностіу сфері цивільного захисту, д.т.н., с.н.с.

Олександр ЛЄВТЄРОВ