



Інститут
кібернетики імені
В.М.Глушкова НАН
України

Київський
національний
університет
імені Т.Шевченка

НТУУ «Київський
політехнічний
інститут імені Ігоря
Сікорського»

Інститут проблем
моделювання в
енергетиці імені
Г.Є.Пухова НАН
України

Оптимізація безпекових ризиків для критичної інфраструктури

Представлено *Інститутом кібернетики імені В.М.Глушкова*
Національної академії наук України

Список авторів:

- 1. АТОЄВ Костянтин Леонович** – кандидат біологічних наук, старший науковий співробітник Інституту кібернетики імені В.М.Глушкова Національної академії наук України;
- 2. ГОРБАЧУК Василь Михайлович** – доктор фізико-математичних наук, професор, завідувачий відділом Інституту кібернетики імені В.М.Глушкова Національної академії наук України;
- 3. ДАНИЛОВ Валерій Якович** – доктор технічних наук, професор, професор кафедри штучного інтелекту Навчально-наукового інституту прикладного системного аналізу Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;
- 4. КИРИЛЮК Володимир Семенович** - доктор фізико-математичних наук, провідний науковий співробітник Інституту кібернетики імені В.М.Глушкова Національної академії наук України;
- 5. КЛЮШИН Дмитро Анатолійович** - доктор фізико-математичних наук, професор, професор кафедри обчислювальної математики факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка;
- 6. КОВАЛЬЧУК Людмила Василівна** – доктор технічних наук, професор, провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.
- 7. НОРКІН Володимир Іванович** - доктор фізико-математичних наук, провідний науковий співробітник Інституту кібернетики імені В.М.Глушкова Національної академії наук України;
- 8. СЕМЕНОВ Володимир Вікторович** - доктор фізико-математичних наук, професор, професор кафедри обчислювальної математики факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка.



Оптимізація безпекових ризиків для критичної інфраструктури

- **Розроблено методологію оптимізації безпекових ризиків** для критичної інфраструктури (КІ), зокрема в паливно-енергетичному секторі, телекомунікаціях, транспорті, фінансах та ЖКГ. Методологія базується на математичному моделюванні безпекових ситуацій в умовах системних ризиків і невизначеностей.
- **Для кількісної оцінки ризиків** застосовано сучасні методи: теорію мір ризику, стохастичне програмування, математичну статистику, системний аналіз, методи дослідження рівноваг і варіаційних нерівностей, машинне навчання та криптоаналіз.
- **Запропоновано нові підходи до оцінки ризиків**, зокрема на основі теорії катастроф, динамічних моделей та поліедральних когерентних мір ризику. Розроблено нові алгоритми для моделювання масоперенесення в пористих середовищах, оцінки екологічних ризиків і оптимального розподілу ресурсів для захисту КІ від терористичних атак і катастрофічних подій.
- **Запропоновано нові методи оцінки стійкості криптоалгоритмів та смарт-контрактів до атак**, а також алгоритми для ігрових моделей захисту КІ.

Результати роботи забезпечують:

- ❖ оцінку стану КІ, прогнозування вразливостей та планування захисту від загроз (терористичних, повітряних, кібератак);
- ❖ оптимальний розподіл захисних ресурсів;
- ❖ мінімізацію наслідків надзвичайних ситуацій;
- ❖ визначення оптимальних стратегій сталого розвитку в умовах збройної агресії РФ, геополітичної турбулентності та кліматичних змін.

Атоєв К.Л.
Горбачук В.М.
Данилов В.Я.
Кирилюк В.С.
Ключин Д.А.
Ковальчук Л.В.
Норкін В.І.
Семенов В.В.



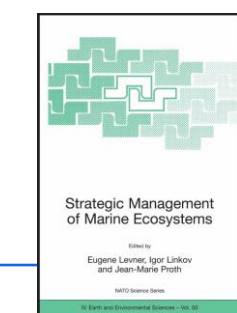
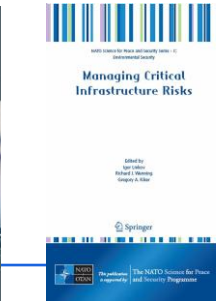
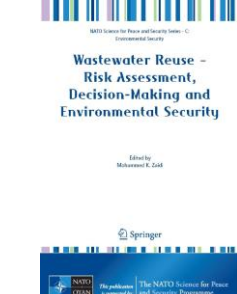
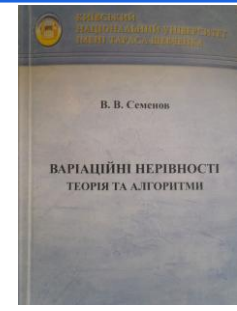
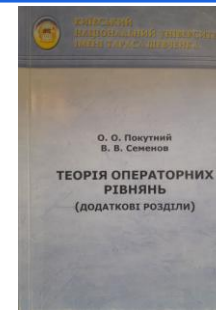
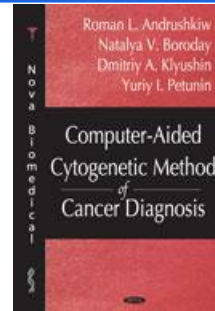
Оптимізація безпекових ризиків для критичної інфраструктури

- Одноосібні монографії – 2
- Колективні монографії – 42
- Видані за кордоном – 27
- Статті в журналах категорії "А" – 147
- Статті у зарубіжних виданнях – 138
- Статі у журналах категорії "Б" – 98

Посилання / h-індекс:

- Web of Science – 1189 / 15,
- Scopus – 1773 / 20,
- Google Scholar 5516 / 30.

- Патенти на корисну модель – 4
- Авторські свідоцтва – 2
- Національні стандарти – 1
- Захищено кан.(д.ф.) / док. діс.– 18 / 2



Публікації,
цитування,
результати.



Моделі та методи дослідження операцій для захисту критичної інфраструктури

Ризик (міра) = Загроза x Уразливість x Втрати

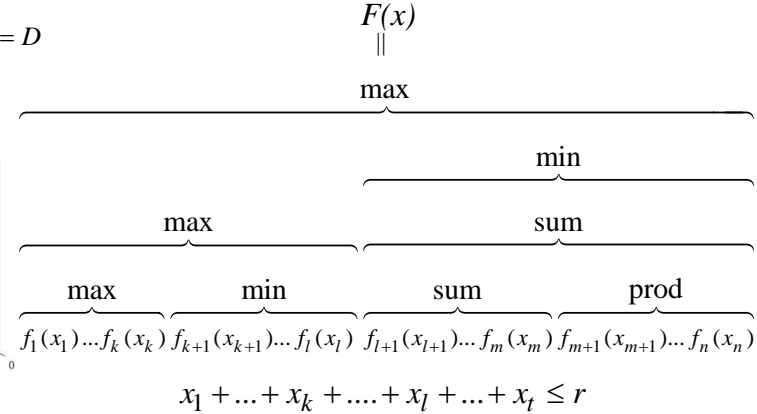
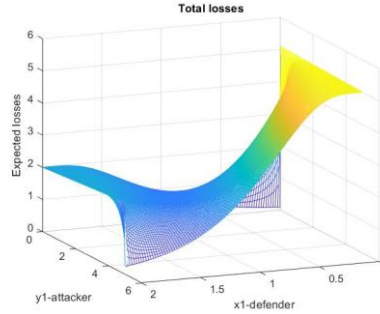
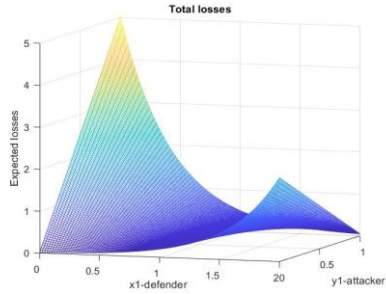


Ієрархічне динамічне програмування для оптимального розподілу захисних ресурсів

$$\min_d \max_a \left[Risk(a, d) = \sum_{k=1}^K C_k a_k (1-p)^{d_k} \right] \quad \min_d \max_a \left[Risk(a, d) = \sum_{k=1}^K C_k \left(1 - \left(1 - (1-p)^{d_k} \right)^{a_k} \right) \right]$$

$$\sum_{k=1}^K a_k = 1 \quad \sum_{k=1}^K d_k = D$$

$$\sum_{k=1}^K a_k = A \quad \sum_{k=1}^K d_k = D$$



ЗАСТОСУВАННЯ МОДЕЛЕЙ ТА МЕТОДІВ ДОСЛІДЖЕННЯ ОПЕРАЦІЙ ДЛЯ ПЛАНУВАННЯ ЗАХИСТУ КІ

Norkin V.I. et al. Models of the optimal resource allocation for the critical infrastructure protection. *Cybernetics and Systems Analysis*, 2018, Vol. 54, No. 5, P.696-706.

Адаптовано математичні *моделі і методи дослідження операцій*, зокрема стохастичні ігри, стохастичні оптимізаційні та моделі ієрархічного динамічного програмування, для планування оптимального розподілу ресурсів для захисту об'єктів критичної інфраструктури від терористичних і масованих повітряних атак та катастрофічних подій.



Когерентні міри ризику (КМР)

A1) $\rho(X+c) = \rho(X) + c, c \in R$

трансляційно інваріантна;

A2) $\rho(X_1 + X_2) \leq \rho(X_1) + \rho(X_2)$

субадитивна;

A3) $\rho(\lambda X) = \lambda \rho(X), \lambda \geq 0$

позитивно однорідна;

A4) $\rho(X_1) \leq \rho(X_2), X_1 \leq X_2$ (за розпод.) монотонна.

$$\rho(X) = \sup_{\zeta \in \mathfrak{M}_\rho} \int_{\Omega} \zeta(\omega) X(\omega) dP_0(\omega) = \sup_{P \in Q_\rho(P_0)} E_P[X]$$

$Q_\rho(P_0)$ – опукла слабо* замкнена множина імовірнісних мір.

Поліедральні КМР (ПКМР) в L_1

$$\mathfrak{M}_\rho = \mathfrak{M}_0; \quad \mathfrak{M}_\rho = \mathfrak{M}_0 \cap \mathfrak{M}_1; \quad \mathfrak{M}_\rho = \mathfrak{M}_0 \cap \mathfrak{M}_2; \quad \mathfrak{M}_\rho = \mathfrak{M}_0 \cap \mathfrak{M}_1 \cap \mathfrak{M}_2, \text{ де}$$

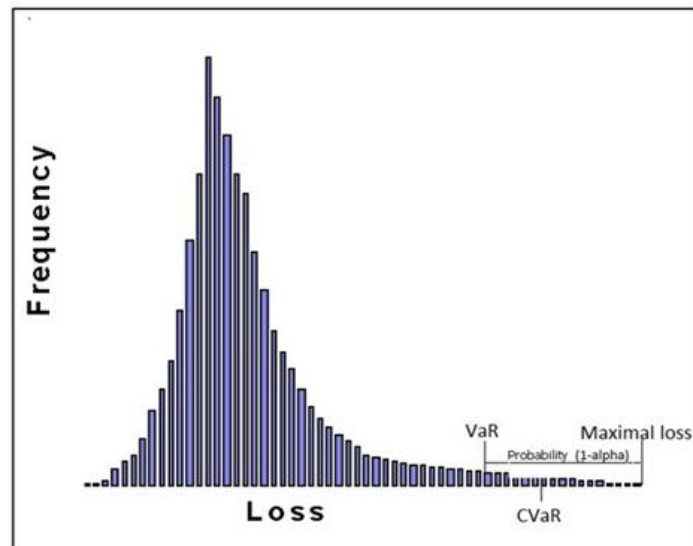
$$\mathfrak{M}_0 = \left\{ \zeta(\cdot) \geq 0 \text{ a.s.}, \int_{\Omega} \zeta(\omega) dP_0(\omega) = 1 \right\},$$

$$\mathfrak{M}_1 = \left\{ \zeta(\cdot): \int_{\Omega} \zeta(\omega) X_i(\omega) dP_0(\omega) \leq c_i, i = 1, \dots, k \right\},$$

$$\mathfrak{M}_2 = \left\{ \zeta(\cdot): \gamma_1 \leq \zeta(\cdot) \leq \gamma_2 \text{ a.s.}, 0 \leq \gamma_1 \leq 1 \leq \gamma_2 \right\}.$$

$$\mathfrak{M}_{CVAR_\alpha} = \left\{ \zeta(\cdot): 0 \leq \zeta(\cdot) \leq \frac{1}{1-\alpha} \text{ a.s.}, \int_{\Omega} \zeta(\omega) P_0(d\omega) = 1 \right\}$$

$$\Rightarrow \mathfrak{M}_0 \cap \mathfrak{M}_2$$



КОГЕРЕНТНІ
ТА
ПОЛІЕДРАЛЬНІ
КОГЕРЕНТНІ
МІРИ РИЗИКУ
В L_1



ПКМР для скінчених дискретно розподілених в.в.

$$\rho(X) = \sup_{P \in Q_\rho(P_0)} E_P[X], \text{ де } Q_\rho(P_0) = \{B(p_0)p \leq c(p_0), p \geq 0\}.$$

де матриця $B_1(p_0)$ та вектор $c_1(p_0)$ описують змістовну частину обмежень, B_0 та c_0 – стандартну.

$$B(p_0) = \begin{pmatrix} B_1(p_0) \\ B_0 \end{pmatrix}, c(p_0) = \begin{pmatrix} c_1(p_0) \\ c_0 \end{pmatrix}, B_0 = \begin{pmatrix} 1 \dots 1 \\ -1 \dots -1 \end{pmatrix}, c_0 = \begin{pmatrix} 1 \\ -1 \end{pmatrix},$$

Приклади:

П1) $\rho(X) = \text{ess sup } X, Q(p_0) = \left\{ 0 \leq p, \sum_{i=1}^n p_i = 1 \right\}$ – максимальні втрати,

П2) $\rho(X) = E[X], Q(p_0) = \left\{ 0 \leq Ip \leq p_0, \sum_{i=1}^n p_i = 1 \right\} = \{p_0\}$ – середні втрати,

П3) $\rho(X) = \text{CVaR}_\alpha(X), Q(p_0) = \left\{ 0 \leq Ip \leq \frac{1}{1-\alpha} p_0, \sum_{i=1}^n p_i = 1 \right\}$ – міра CVaR,

П4) $\rho(X) = -S_u(-X), Q(p_0) = \left\{ \gamma_1 p_0 \leq Ip \leq \gamma_2 p_0, \sum_{i=1}^n p_i = 1 \right\}, 0 \leq \gamma_1 \leq 1 \leq \gamma_2$ –

оптимізований еквівалент визначеності.

Робастні конструкції мір ризику за невизначеності $P_0 \in AS$

$$P_0 \in AS \Rightarrow \rho_{AS}(X) = \sup_{P_0 \in AS} \sup_{P \in Q_\rho(P_0)} E_P[X] = \sup_{P \in Q_\rho(AS)} E_P[X].$$

Робастні конструкції ПКМР для дискретно розподілених в.в.

$$\rho_{AS}(X) = \sup_{P \in Q_\rho(AS)} E_P[X], \text{ де } Q_\rho(AS) = \{B(p_0)p \leq c(p_0), p_0 \in AS, p \geq 0\}.$$



Оптимізація при невизначеності: при відомій P_0 та за наявності множини AS

$$\begin{aligned}
 f_0(x, \omega) \rightarrow \min_{x \in M} & \Rightarrow 1) \rho_0(f_0(x, \cdot)) \rightarrow \min_{x \in M} & \Rightarrow 2) \rho_{0; AS}(f_0(x, \cdot)) \rightarrow \min_{x \in M} \\
 f_i(x, \omega) \leq 0, i = 1, \dots, m & \Rightarrow \rho_i(f_i(x, \cdot)) \leq 0, i = 1, \dots, m & \Rightarrow \rho_{i; AS}(f_i(x, \cdot)) \leq 0, i = 1, \dots, m \\
 \omega \in \Omega & &
 \end{aligned}$$

Середні та найгірші значення, CVaR, інші варіанти ПКМР. Імовірнісні функціонали апроксимуються через CVaR:

$$P\{\omega: f_i(x, \omega) \leq 0\} \geq \alpha_i \Leftrightarrow VaR_{\alpha_i}(f_i(x, \omega)) \leq 0 \Rightarrow CVaR_{\alpha_i}(f_i(x, \omega)) \leq 0.$$

Стохастична, Робастна та Робастна за Розподілом Оптимізація в рамках *єдиного підходу*: CO&PO зводяться до 1); PPO – до 2).

**ОПТИМІЗАЦІЯ
ПРИ НЕВИЗНАЧЕ-
НОСТІ:
СТОХАСТИЧНА,
РОБАСТНА ТА
РОБАСТНА ЗА
РОЗПОДІЛОМ**

Таке зведення дозволяє врахувати в конструкціях ПКМР потрібні властивості отримуваних рішень: *робастність* до невизначеності та *ефективність* за критеріями. Лінійні проблеми з невизначеністю зводяться до відповідних задач лінійного програмування. Зокрема, до них зведені різноманітні задачі оптимізації портфеля за співвідношенням винагорода-ризик.

Результати для кількісного оцінювання ризику та їх застосування в задачах оптимізації при невизначеності отримані на рівні світових стандартів.

Вони застосовні до проблем захисту критичної інфраструктури від природних та техногенних загроз, а також від терористичних загроз при аналізі ризику з противником для пошуку ефективних (оптимальних) рішень.



Дослідження впливу кліматичних змін на стан критичної інфраструктури (КІ)

Atoyev K.L., Knopov P.S. Mathematical modeling of climate change impact on relationships of economic sectors. *Cybern. Syst. Analysis*, 2023, 59(4), pp.: 535–545, <https://doi.org/10.1007/s10559-023-00589-9>

$$\varepsilon_c \frac{dC}{dt} = a_0 + (a_1 + \sum_{i=1}^5 k_i X_i) E - a_2 C (b_0 + G),$$

$$\frac{dG}{dt} = F_G(X_6) - a_3 G (c_0 + \sum_{i=1}^6 c_i X_i),$$

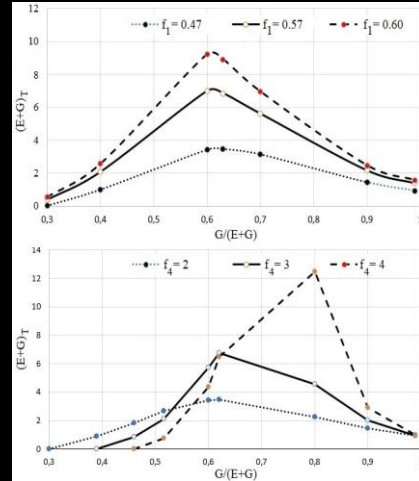
$$\frac{dE}{dt} = F_E(X_1) - a_4 E (d_0 + \sum_{i=1}^6 d_i X_i),$$

$$\varepsilon_{ix} \frac{dX_i}{dt} = \sigma_i(C)(Y_i - X_i),$$

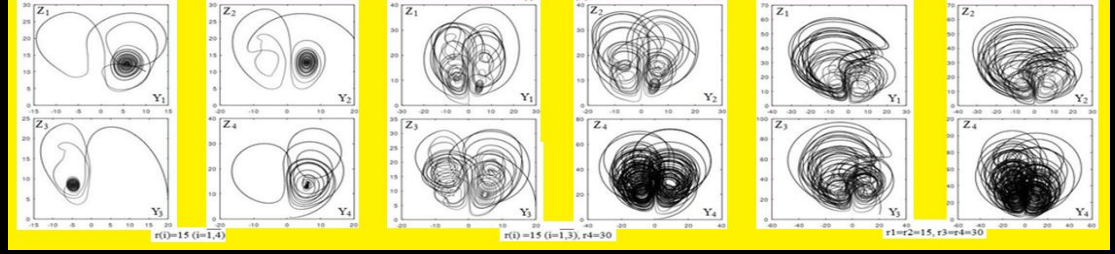
$$\varepsilon_{iy} \frac{dY_i}{dt} = [r_i(1 - \sum_{i=1, i \neq j}^6 a_{ij} X_j) - Z_i] X_i - Y_i,$$

$$\varepsilon_{iz} \frac{dZ_i}{dt} = X_i Y_i - b_i(C) Z_i,$$

де C — рівень ПІ; E та G — рівні функціонування звичайної та зеленої енергетики відповідно; ε — частка зеленої енергетики у загальному енергетичному балансі;

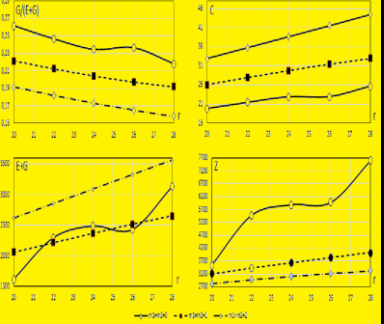


Залежність стаціонарного рівня $E+G$ від величин ε



X_i — нормований рівень продуктивності, Y_i — нормована кількість робочих місць, Z_i — нормований рівень порушень для добувної ($i=1$) та переробної ($i=2$) промисловостей; агропромислового комплексу ($i=3$), систем постачання електроенергії, газу, пари та кондиціонуваного повітря ($i=4$), транспорту та системи ЖКХ ($i=5$); сектору відтворення зеленої енергетики ($i=6$);

Параметр r характеризує баланс між попитом та пропозицією на продукцію виробничих систем та кількості зайнятих робочих місць.



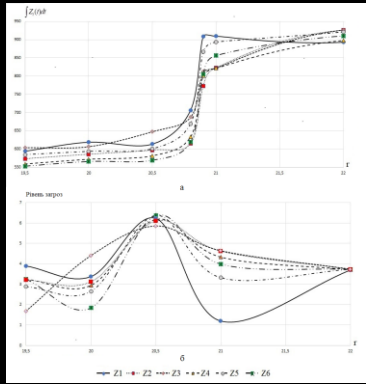
Зміна стаціонарних рівнів частки зеленої енергетики у енергетичному балансі, сумарних обсягів продукції, яка створюється традиційною та зеленою енергетиками, парникових газів та порушень при варіації параметра r

$$F(\sigma_i, r_i, b_i) = \sum_{i=1}^6 k_{si} I_{si} + \sum_{i=1}^6 k_{zi} I_{zi} + \frac{k_{eg} I_{eg}}{I_{eg}} + k_c I_{ec},$$

$$I_{si} = \int_0^T X_i dt, \quad I_{zi} = \int_0^T Z_i dt, \quad I_{ec} = \int_0^T C dt,$$

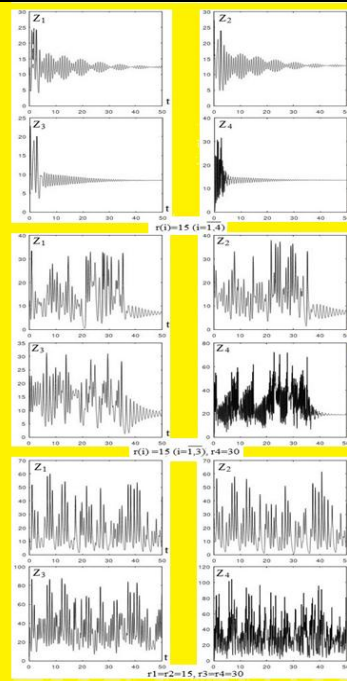
$$I_{eg} = \int_0^T E dt + \int_0^T G dt,$$

Визначення ефективних керувань для мінімізації порушень Z , рівня ПІ та максимізації рівня якості життя



Рівні сумарних порушень (а) та загроз (б) у секторах КІ у разі варіацій параметрів r

Фазовий портрет моделі



Динаміка змін порушень у 8 різних секторах КІ у разі варіацій параметрів r



Кожний сектор КІ розглядають у термінах нормованого рівня продуктивності (X_i), нормованої кількості робочих місць (Y_i) і нормованого рівня структурних порушень (Z_i) для продовольчого ($i=1$), логістичного ($i=2$) та медико-соціального ($i=3$) секторів економіки відповідно.

$$\varepsilon_i \frac{dX_i}{dt} = \sigma_i(Y_i - X_i) + \delta_i w_{ij}, \quad \varepsilon_i \frac{dY_i}{dt} = [r_i - Z_i]X_i - Y_i + \delta_i w_{ij}, \quad \varepsilon_i \frac{dZ_i}{dt} = X_i Y_i - b_i Z_i + \delta_i w_{ij},$$

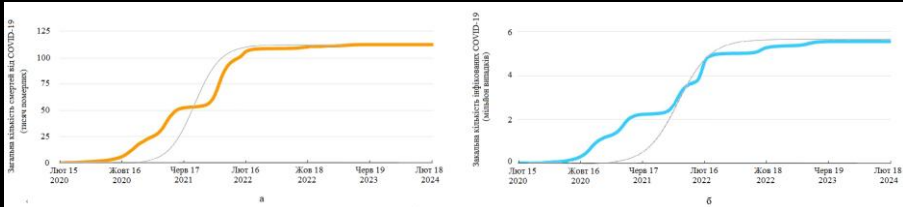
$$\frac{dy_1}{dt} = \frac{R(Z_3)y_1 y_2}{NT_{inf}} + \alpha(t)y_3 + \beta_1 w_1, \quad \frac{dy_2}{dt} = \frac{R(Z_3)y_1 y_2}{NT_{inf}} - \frac{U_1(X_3)y_2}{NT_m} + \beta_2 w_2,$$

$$\frac{dy_3}{dt} = (1 - \alpha_0) \frac{U_1(X_3)y_2}{NT_m} - \alpha(t)y_3 + \beta_3 w_3, \quad \frac{dy_4}{dt} = \alpha_0 \frac{U_1(X_3)y_2}{NT_m} + \beta_3 w_4,$$

$$R(Z_3) = R(1 + Z_3 / k_1), \quad U_1(X_3) = 1 + k_2 X_3^2 / (k_3 + X_3^2), \quad U_2(y_2) = 1 + l_1 y_2 / N,$$

де y_1 — здорові особи; y_2 — інфіковані особи; y_3 — особи, які одужали; y_4 — померлі особи; β_i ($k = \overline{1,4}$) — параметри інтенсивності збуджень; $w_i(t)$ має той самий сенс, що в моделі (1), та відповідає тим самим умовам; α_0 — частина померлих осіб; T_{inf} — активний період, протягом якого хворий є заразним; T_m — середній період одужання хворого; N — загальна кількість населення.

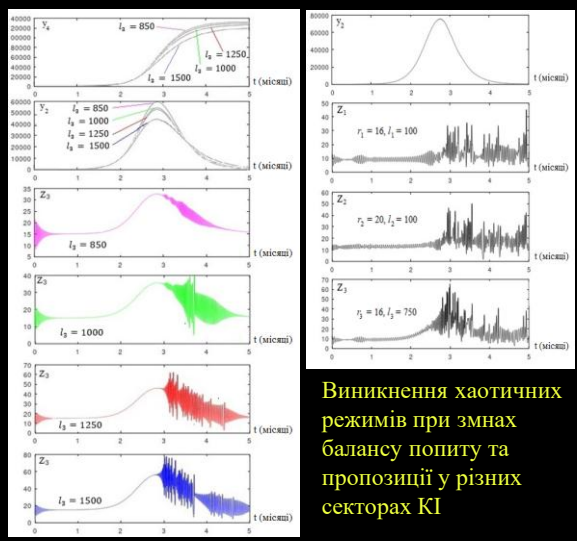
Модель, яка включає епідемічний, продовольчий, транспортний та медичний сектори КІ та систему взаємозв'язків між ними за допомогою якої проведено дослідження взаємозв'язків між динамікою розвитку пандемії COVID-19 та станом КІ. Кожний з секторів розглядається з точки зору рівня продуктивності, кількості робочих місць та структурних порушень. Проведено дослідження впливу пандемії COVID-19 на зміни балансу попиту та пропозиції в секторах економіки, пов'язаних з виробництвом, транспортом та медичною сферою.



Зіставлення результатів моделювання (тонка лінія) з наявними даними щодо динаміки пандемії в Україні (жирна лінія).

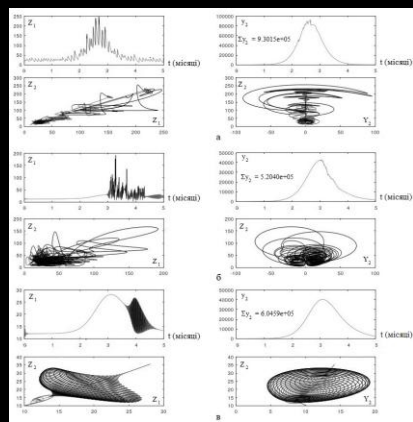
Дослідження впливу пандемії COVID-19 на стан критичної інфраструктури (КІ)

Atoyev K.L., Knopov P.S. Mathematical modeling of the economic impacts of the COVID-19 pandemic Cybern. Syst. Analysis, 2024, 60(5), pp.: 759–769, <https://doi.org/10.1007/s10559-024-00713-3>

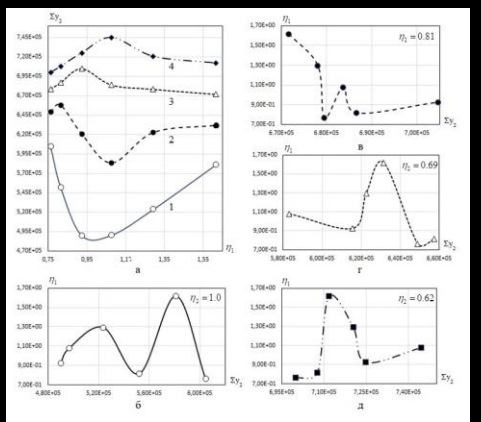


Виникнення хаотичних режимів при змнах балансу попиту та пропозиції у різних секторах КІ

Виникнення хаотичних режимів при збільшенні впливу пандемії на медичний сектор КІ



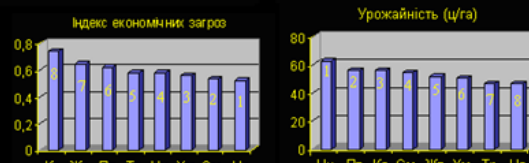
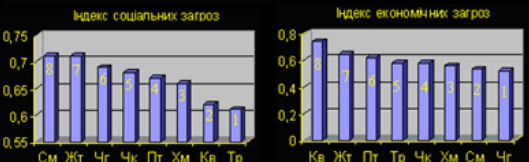
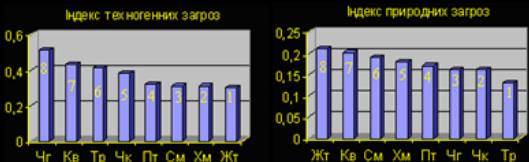
Зміни рівня інфікованих та рівнів структурних порушень у разі варіації параметрів b (зменшення рівня пропозиції робочих місць у секторах КІ



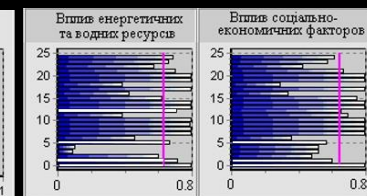
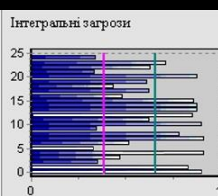
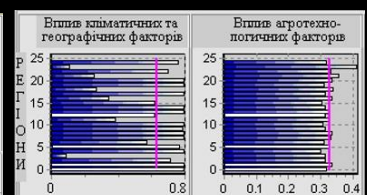
Залежність загальної кількості інфікованих та відносних змін рівня пропозиції робочих місць \tilde{y}_1 за різних рівнів співвідношень попиту та пропозиції (а); обернена залежність \tilde{y}_2 від рівня інфікованих при різних рівнях співвідношення попиту та пропозиції \tilde{y}_1 (б-д).



РАНЖУВАННЯ ПАРАМЕТРІВ, ЩО ВИЗНАЧАЮТЬ ІНВЕСТИЦІЙНУ ПРИВАБЛИВІСТЬ РЕГІОНІВ УКРАЇНИ

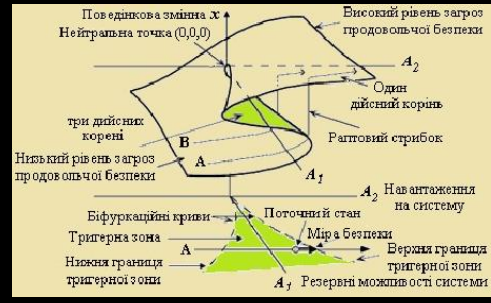


Житомирщина (Жт) Київщина (Кв) Полтавщина (Пт) Сумщина (См)
Тернопільщина (Тр) Хмельницька (Хм) Черкащина (Чк) Чернігівщина (Чг)



За допомогою теорії катастроф розроблено метод оцінювання ризиків для продовольчої безпеки та управління ними, який ґрунтується на використанні даних щодо достатності споживання I_1 , диференціації вартості продуктів харчування за соціальними групами населення I_2 , добової енергетичної цінності раціону людини I_3 , доступності продуктів харчування I_4 , обмеженнями економічної діяльності у зв'язку з епідемією COVID-19 I_5 , скороченням посівних площ та порушенням транспортних ланцюгів внаслідок широкомасштабних військових конфліктів I_6 . За допомогою моделі проведено комплексна оцінка інвестиційної привабливості деяких аграрних регіонів в умовах зростання невизначеності та ризиків.

1	2	3	4	5
Crimea	Уманська	Волинська	Дніпропетровська	Донецька
АР Крим	Вінницька	Львівська	Дніпропетровська	Донецька
Закарпатська	Закарпатська	Закарпатська	Закарпатська	Закарпатська
11	12	13	14	15
Житомирська	Закарпатська	Закарпатська	Закарпатська	Закарпатська
16	17	18	19	20
Київська	Львівська	Львівська	Львівська	Львівська
21	22	23	24	25
Хмельницька	Хмельницька	Хмельницька	Хмельницька	Хмельницька



Оцінювання ризиків продовольчої безпеки та інвестиційної привабливості аграрних регіонів України

Kpovov, K., Ermolieva, T., Kpovov, P. (2024). Mathematical Modeling of Interconnections Between Ecological, Food, and Economic Dimensions of Security. In: Zagorodny, A., Bogdanov, V., Zaporozhets, A. (eds) Nexus of Sustainability. Studies in Systems, Decision and Control, vol 559. Springer, Cham. P.185-209. https://doi.org/10.1007/978-3-031-66764-0_2

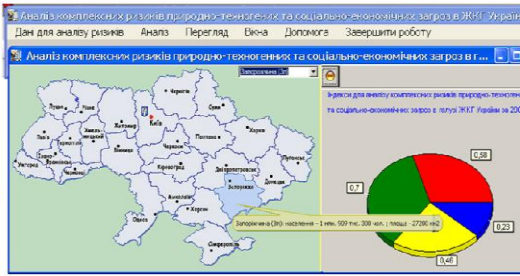
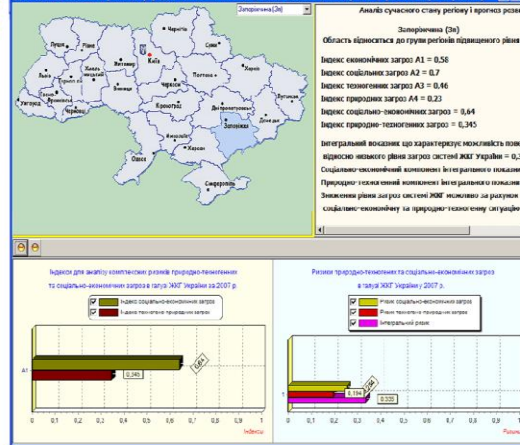
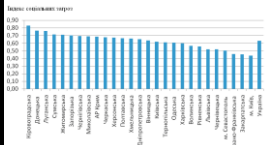
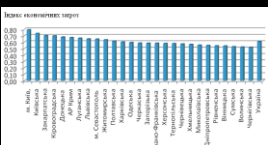
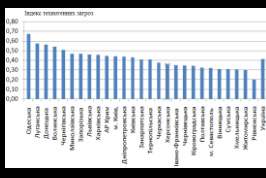
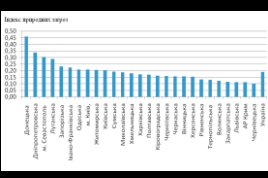
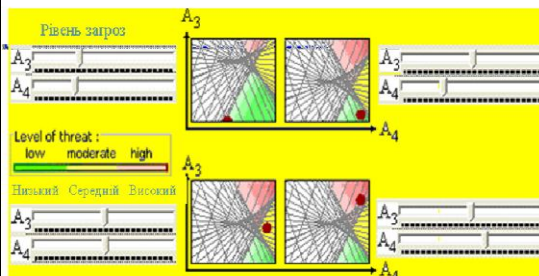
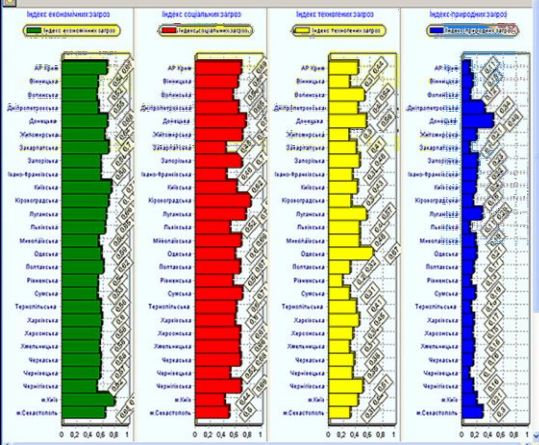
$$-\frac{\partial U(x)}{\partial x} = x^3 + A_1x + A_2 = 0 \quad \Delta = 4A_1^3 - 27A_2^2 \quad A_1 = a_0 + a_1I_1 + \dots + a_6I_6, \quad A_2 = b_0 + b_1I_1 + \dots + b_6I_6$$

Показник/Регіон	Жт	Кв	Пт	См	Тр	Хм	Чк	Чг
Техногенні загрози (X_1)	1	7	4	3	6	2	5	8
Природні загрози (X_2)	8	7	4	6	1	5	2	3
Соціальні загрози (X_3)	7	2	4	8	1	3	5	6
Економічні загрози (X_4)	7	8	6	2	5	3	4	1
Сталість урожаю (X_5)	4	1	8	6	5	3	7	2
Урожайність (X_6)	5	3	2	4	7	6	1	8
I_2 ($\nu_2 = 0,15; i=1,4; \nu_2 = 0,2; i=5,6$)	5,25	4,4	4,7	4,85	4,35	3,75	4,0	4,7
Ранг III	8	4	5-6	7	3	1	2	5-6
I_3 ($\nu_3 = 0,1; i=1,4; \nu_3 = 0,3; i=5,6$)	5,0	3,6	4,8	4,9	4,9	4,0	4,0	4,8
Ранг III	8	1	4-5	6-7	6-7	2-3	2-3	4-5
I_5 ($\nu_5 = 0,05; i=1,4; \nu_5 = 0,4; i=5,6$)	4,75	2,8	4,9	4,95	5,45	4,25	4,0	4,9
Ранг III	4	1	5-6	7	8	3	2	5-6

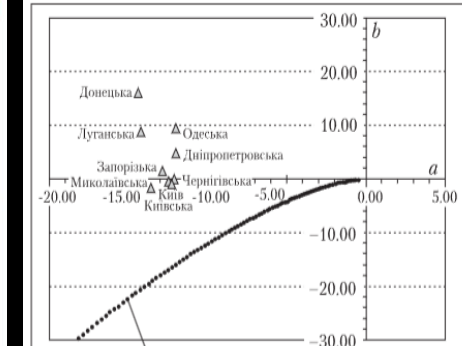


Оцінювання комплексних ризиків у секторі ЖКГ

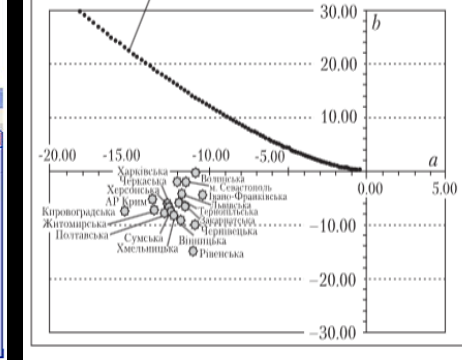
Пепеляев В.А., Кнопов П.С., Атоев К.Л., Бігдан В.Б., Чорний Ю.М. Інформаційно-аналітична система для аналізу комплексних ризиків природно-техногенних та соціально-економічних загроз в галузі житлово-комунального господарства України. *Наука та інновації*. 2010. Т. 6, № 3. С. 39—46. <https://scinn.org.ua/sites/default/files/pdf/2010/N3/Pepelyaev.p.pdf>



Розроблено інформаційну систему для оцінки комплексних ризиків природно-техногенних та соціально-економічних загроз в системі ЖКГ, яка дає можливість: 1) оцінювати деформації простору безпеки в умовах підвищення невизначеності; 2) досліджувати динаміку ризику надзвичайних ситуацій як функцію техногенних, екологічних, соціальних та економічних змінних; 3) оцінювати ризик природно-техногенних та соціально-економічних надзвичайних ситуацій для аналізу поточної ситуації та прийняття управлінських рішень



Біфуркаційні криві, що розділяють зони підвищеного та відносно низького рівня загроз



Проекція поверхні станів системи ЖКГ параметрів управління **a** та **b**, які характеризують відповідно соціально-економічні та природно-техногенні загрози. Було проведено обчислення інтегральних ризиків переходу регіонів з групи відносно низького рівня загроз у групу підвищеного рівня загроз R_I , а також їх соціально-економічних R_{se} та їх природно-техногенних R_{pt} складових.



Зміни організаційної стійкості



Підхід до підтримки прийняття рішень для підвищення стійкості (резильентності) (галузевих, регіональних або глобальних) критичних інфраструктур



Алгоритм підвищення стійкості (резильентності) критичних інфраструктур



Міждисциплінарний підхід для взаємопов'язаних критичних інфраструктур



Моделі та методи децентралізації для оптимізації безпекових ризиків критичних інфраструктур



Варіаційна нерівність: find $x \in C$ such that $(\forall x, y - x) \geq 0 \quad \forall y \in C$.

Algorithm 1. Extrapolation from the Past with adaptive step size.

Initialization. Select $y_0 \in E, x_0 \in \text{int dom } \omega, \tau \in (0, \frac{1}{3})$ and a real number $\lambda_1 > 0$.
Set $n \leftarrow 1$.

1) Compute

$$y_n = P_{x_n}^C(-\lambda_n V y_{n-1}).$$

2) Compute

$$x_{n+1} = P_{x_n}^C(-\lambda_n V y_n).$$

3) If $y_n = x_n = x_{n+1}$, then STOP and $x_{n+1} \in S$, otherwise compute

$$\lambda_{n+1} = \begin{cases} \min \left\{ \lambda_n, \tau \frac{\|y_n - y_{n-1}\|}{\|V y_n - V y_{n-1}\|_*} \right\}, & \text{if } V y_n \neq V y_{n-1}, \\ \lambda_n, & \text{otherwise.} \end{cases}$$

Set $n \leftarrow n + 1$ and go to 1.

$$\max_{i=1, \dots, m} f_i(x) \rightarrow \min_x$$

\Downarrow

$$\min_x \max_{y \in \Delta^m} \left(\sum_{i=1}^m y_i f_i(x) \right)$$

$$F(Kx) + G(x) \rightarrow \min_x$$

\Downarrow

$$\min_x \max_y (\langle Kx, y \rangle + G(x) - F^*(y))$$

$$\left(\left(\begin{array}{c} \nabla_x f(x^*, y^*) \\ \nabla_y g(x^*, y^*) \end{array} \right), \left(\begin{array}{c} x - x^* \\ y - y^* \end{array} \right) \right) \geq 0 \quad \forall (x, y) \in X \times Y$$

$$\left(\left(\begin{array}{c} \nabla_x F(x^*, y^*) \\ -\nabla_y F(x^*, y^*) \end{array} \right), \left(\begin{array}{c} x - x^* \\ y - y^* \end{array} \right) \right) \geq 0 \quad \forall (x, y) \in X \times Y$$

Adversarial Learning

$$\min_x \mathbb{E}_{(u, v)} \left(\max_{y \in S} L(u + y, v, x) \right)$$

Generative adversarial networks

Algorithm 2. Operator extrapolation with adaptive step size.

Initialization. Select $x_0 \in E, x_1 \in \text{int dom } \omega, \tau \in (0, \frac{1}{2})$ and a real numbers $\lambda_0, \lambda_1 > 0$. Set $n \leftarrow 1$.

1) Compute

$$x_{n+1} = P_{x_n}^C(-\lambda_n V x_n - \lambda_{n-1} (V x_n - V x_{n-1})).$$

2) If $x_{n-1} = x_n = x_{n+1}$, then STOP and $x_{n+1} \in S$, otherwise compute

$$\lambda_{n+1} = \begin{cases} \min \left\{ \lambda_n, \tau \frac{\|x_{n+1} - x_n\|}{\|V x_{n+1} - V x_n\|_*} \right\}, & \text{if } V x_{n+1} \neq V x_n, \\ \lambda_n, & \text{otherwise.} \end{cases}$$

Set $n \leftarrow n + 1$ and go to 1.

Застосування апарату в варіаційних нерівностях для пошуку рішень в ігрових моделях



Розроблено нові, у тому числі адаптивні, алгоритми для варіаційних нерівностей. Ітерації даних алгоритмів дешевші за ітерацію екстраградієнтного алгоритму за кількістю обчислень значень оператора: одне проти двох.

Розроблені алгоритми орієнтовані на застосування для розв'язання обернених задач, що зв'язані з оцінкою екологічних ризиків, негладких задач регресії, задач навчання генерувальних змагальних нейронних мереж (GANs) та для пошуку рішень в ігрових моделях захисту критичної інфраструктури.

Розроблено нові алгоритми з дивергенцією Брегмана та алгоритми для розв'язання варіаційних нерівностей в 2-рівномірно опуклих та рівномірно гладких банахових просторах, що використовують проєкцію Альбера замість метричної.

Розроблено нові алгоритми для дворівневих варіаційних нерівностей, що поєднують ідею ітераційної регуляризації з апроксимацією Браудера-Тихонова.

Розроблено адаптивні алгоритми для задач про рівновагу у різних просторах.

**Застосування
апарату в
варіаційних
нерівностей для
пошуку рішень в
ігрових моделях**



find $x \in C$ such that $F(x, y) \geq 0 \quad \forall y \in C$.

$$\begin{cases} y_n = \text{prox}_{\lambda_n F(x_n, \cdot)} x_n = \arg \min_{y \in C} \left(F(x_n, y) + \frac{1}{2\lambda_n} d^2(y, x_n) \right), \\ x_{n+1} = \text{prox}_{\lambda_n F(y_n, \cdot)} x_n = \arg \min_{y \in C} \left(F(y_n, y) + \frac{1}{2\lambda_n} d^2(y, x_n) \right), \end{cases}$$

$$\begin{cases} y_n = \text{prox}_{\lambda_n F(y_{n-1}, \cdot)} x_n = \arg \min_{y \in C} \left(F(y_{n-1}, y) + \frac{1}{2\lambda_n} d^2(y, x_n) \right), \\ x_{n+1} = \text{prox}_{\lambda_n F(y_n, \cdot)} x_n = \arg \min_{y \in C} \left(F(y_n, y) + \frac{1}{2\lambda_n} d^2(y, x_n) \right). \end{cases}$$

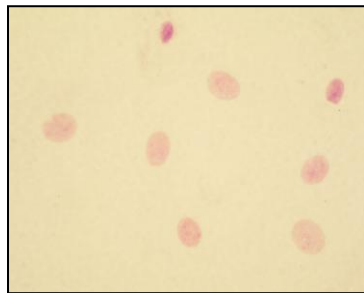
Отримано теореми збіжності та оцінки швидкості збіжності. Усі отримані результати на рівні існуючих у світі аналогів або кращі.

Переваги результатів роботи перед існуючими полягають в більш завершених і конструктивних математичних результатах, що стосуються практично важливих класів математичних моделей.

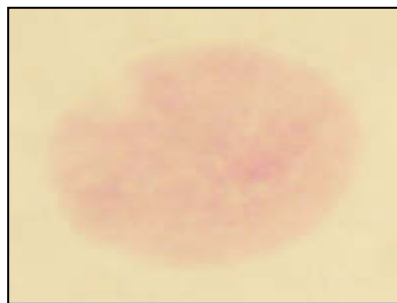
Використання теоретичних результатів в навчальному процесі Київського національного університету імені Тараса Шевченка (теми дисертацій аспірантів та магістрів) вже дозволяє готувати для України фахівців-аналітиків, які володіють алгоритмічним апаратом для сучасних ігрових моделей захисту критичної інфраструктури.

**Застосування
апарату в
варіаційних
нерівностях для
пошуку рішень в
ігрових моделях**

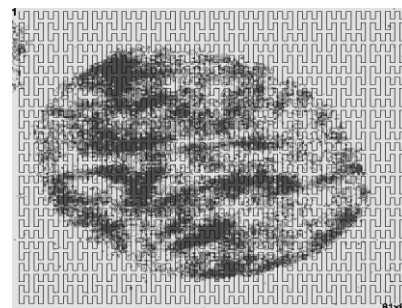
Оцінювання індивідуального ризику раку молочної залози



ДНК кількох ядер, забарвлених за Фьольгеном



ДНК одного ядра, забарвленого за Фьольгеном



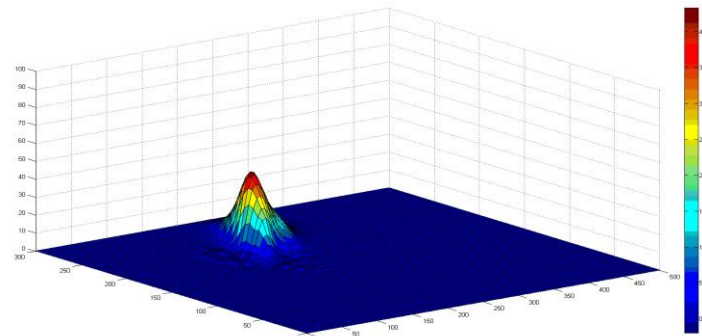
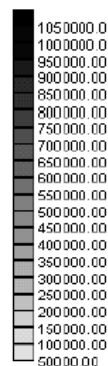
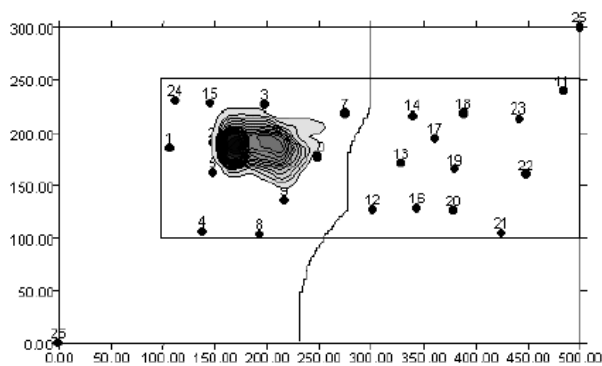
Оцінка фрактальної розмірності ядра за допомогою кривої Гільберта

Чутливість = 94%, специфічність = 96%

ОЦІНЮВАННЯ
ІНДИВІДУАЛЬНОГО
РИЗИКУ ДЛЯ
СТАНУ ОБ'ЄКТА

МЕТОДИ
РОЗВ'ЯЗУВАННЯ
ПРЯМИХ І
ОБЕРНЕНИХ
ЗАДАЧ ДЛЯ
ОЦІНЮВАННЯ
ЕКОЛОГІЧНОГО
РИЗИКУ

Визначення розташування і потужності джерела радіоактивного забруднення

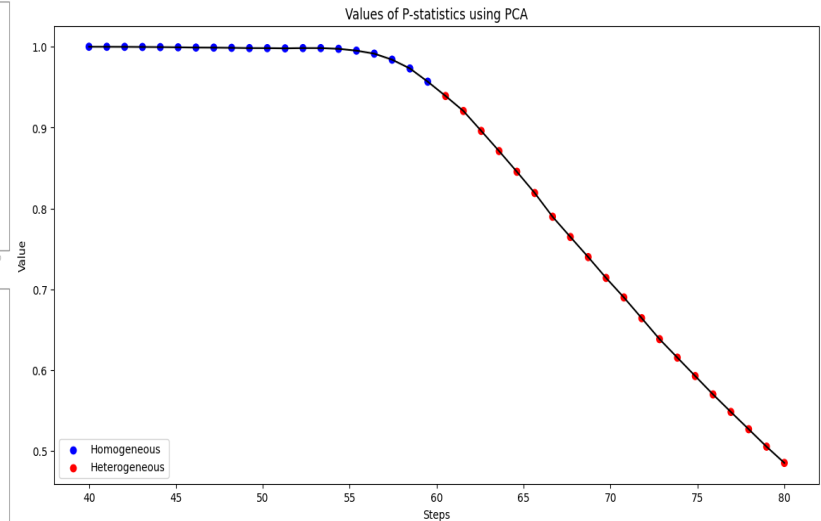
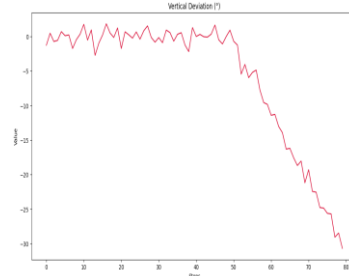
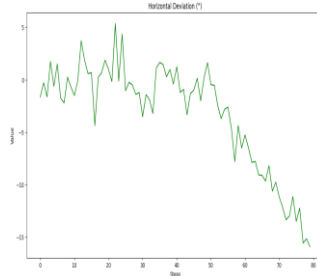
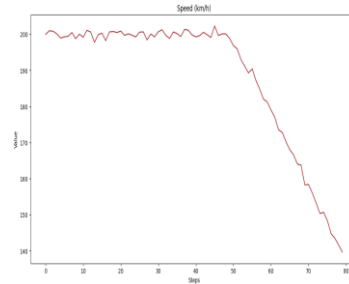
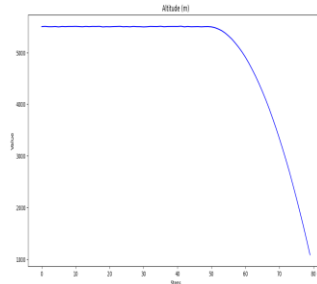




Ідентифікація точок зміни в часових рядах (перехоплення БПЛА)

Інтервал часу, хв	Висота, м	Швидкість км/год	Горизонтальн е відхилення °	Вертикальн е відхилення
0-49 нормальний стан	$N(5500,3)$	$N(200,1)$	$N(0,2)$	$N(0,1)$
50-79 захоплення	Зміна розподілу			

**МЕТОДИ
ІДЕНТИФІКАЦІЇ
ЗМІНИ СТАНУ
ОБ'ЄКТІВ
КРИТИЧНОЇ
ІНФРАСТРУКТУРИ**





**ЗАСТОСУВАННЯ
ТЕОРІЇ
УЗАГАЛЬНЕНИХ
МАРКОВСЬКИХ
ШИФРІВ ДЛЯ
ОЦІНЮВАННЯ
СТІЙКОСТІ
НАЦІОНАЛЬНИХ
СТАНДАРТІВ
БЛОКОВОГО
ШИФРУВАННЯ**

Верхні оцінки теоретичної стійкості
ДСТУ 7624:2024 «Калина» до
різницевого криптоаналізу

$$\max_{\alpha, \beta \in \mathbb{F}_n \setminus \{0\}} \{d_{\alpha, \beta}^{(\mathfrak{A}^{1, r-1})}(\alpha, \beta)\} \leq \begin{cases} 2^{-80}, & \text{при } n = 128; \\ 2^{-160}, & \text{при } n = 256; \\ 2^{-320}, & \text{при } n = 512. \end{cases}$$

Верхні оцінки практичної
стійкості ДСТУ
ГОСТ 28147:2009

Theorem 1. Let \mathfrak{A} be a GOST-like cipher. Then $M_D(\mathfrak{A}) \leq \Delta(\mathfrak{A})^{\lceil \frac{2r}{3} \rceil}$.

Moreover, if $\{Az: z \in W\} \cap W = \{0\}$, then

$$M_D(\mathfrak{A}) \leq \max\{\Delta(\mathfrak{A})^{r-1}, \Delta(\mathfrak{A})^{r+1-2\lceil \frac{r}{3} \rceil} \Delta'(\mathfrak{A})^{\lceil \frac{r}{3} \rceil}\}.$$

СЕКТОР ЦИФРОВИХ ТЕХНОЛОГІЙ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Вперше у світі було **введено поняття узагальненого марковського блокового шифру** та розроблено методи оцінювання стійкості таких шифрів до основних атак.

Отримані **методи були застосовані до діючих стандартів ДСТУ 7624:2014** (та його прообразу шифру «Калина»), а також до ДСТУ ГОСТ 28147:2009, що дозволило:

- вперше отримано науково обґрунтовані оцінки стійкості алгоритмів, реалізованих що використовуються в цих стандартах;
- визначити параметри та їх характеристики, від яких залежать оцінки стійкості;
- вибирати параметри алгоритму, при яких імовірність успіху атаки буде менша за наперед задану нехтувано малу величину.



**РОЗРОБКА НОВИХ
СТАНДАРТІВ
ШИФРУВАННЯ
КОРОТКИХ
ПОВІДОМЛЕНЬ,
ЦИФРОВОГО
ПІДПИСУ,
АВТЕНТИФІКАЦІЇ
НА КРИВИХ
ЕДВАРДСА**

1. Choose a random integer $\varepsilon: 1 < \varepsilon < n-1$.
2. Compute the point $R = \varepsilon P = (x_R, y_R)$, set r as a bit representation of x_R of the length $l(p)$.
3. Compute the point $T = \varepsilon Q = (x_T, y_T)$ and set $\kappa = x_T^{(l)}$ - the lowest l bit of x_T .
4. Compute $t = E_{i,k}^{(\kappa)}(M)$.
5. The ciphertext is $C = (r || t)$.

1. Compute $u = (1-r^2)(a-dr^2)^{-1} \bmod p$ and root $y = \sqrt{u} \bmod p$, set $R = (r, y)$.
2. Compute $T' = (x_{T'}, y_{T'}) = eR'$ and set $x_{T'}^{(l)}$ - the lowest l bit of $x_{T'}$.
3. Compute the message $M = D_{i,k}^{(\kappa)}(t)$.

СЕКТОР ЦИФРОВИХ ТЕХНОЛОГІЙ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Отримано наукові результати у галузі аналізу та синтезу криптосистем на кривих Едвардса, які є удосконаленням існуючих.

Отримані результати дозволили:

- розробити вимоги до параметрів таких криптосистем;
 - розробити прості алгоритми перевірки цих умов;
 - розробити алгоритми генерації цих параметрів.
-
- Розроблено та прийнято Національний стандарт шифрування коротких повідомлень на скручених кривих Едвардса ДСТУ 9041:2020.
 - Розроблено проект стандарту цифрового підпису на скручених кривих Едвардса.
 - Розроблено проект стандарту автентифікації на скручених кривих Едвардса.



Algorithm 1. Tests' independence verification based on the sample correlation matrix Chernoff inequality.

Input: number of tests m ;
number of tests n ;
set of tests $T = \{T_1, \dots, T_m\}$;
set of sequences $\{X^{(j)}\}_{j=1}^n$;
significance level α for testing sequences;
significance level β for verifying hypothesis H_0 .

Step 1. Calculate $\mu = n \cdot (1 - \alpha)^m$ and $\delta_\beta = \sqrt{\frac{3}{\mu} \cdot \ln \frac{2}{\beta}}$.

Step 2. Calculate $C = \delta_\beta \cdot \mu$.

Step 3. Applying tests from the suit to input sequences, find the number k of sequences, which passed all tests.

Step 4. Calculate credential interval as

$$(I_1, I_2) = (\mu - C, \mu + C).$$

Step 5. If $k \in (I_1, I_2)$, then H_0 is accepted, otherwise it is rejected.

Output: "1" for accept, "0" for reject.

СЕКТОР ЦИФРОВИХ ТЕХНОЛОГІЙ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Вперше у світі **формалізоване поняття незалежності статистичних тестів**, що використовуються для перевірки криптографічних якостей ГВП/ГПВП та їх окремих послідовностей, призначених для формування ключових даних та/або параметрів криптосистем.

Розроблено методи та методики перевірки незалежності статистичних тестів та формування набору незалежних статистичних тестів.

Отримані методики застосовано до існуючих наборів тестів (NIST, тощо); показано, що вони виявляють «зайві» тести, узгоджуються з існуючими підходами та дозволяють знизити час тестування до 30%, що дозволяє швидше проводити статистичні дослідження та формувати ключові дані.

МЕТОДИ
СТВОРЕННЯ
НАБОРІВ
НЕЗАЛЕЖНИХ
СТАТИСТИЧНИХ
ТЕСТІВ ДЛЯ
ПЕРЕВІРКИ
КРИПТОГРАФІЧНИХ
ЯКОСТЕЙ
ГВП/ГПВП ТА ЇХ
ПОСЛІДОВНОСТЕЙ



**МАТЕМАТИЧНІ
МОДЕЛІ АТАК НА
СМАРТ-
КОНТРАКТИ, ЩО
ЗАБЕЗПЕЧУЮТЬ
P2P-ПРОДАЖ
ЕЛЕКТРОЕНЕРГІЇ,
ТА НА БЛОКЧЕЙН,
В ЯКОМУ ВОНИ
ФУНКЦІОНУЮТЬ;
ОЦІНКА
ІМОВІРНОСТІ АТАК**

Theorem 3. *The probability $P(z)$ of double spend attack after z confirmation blocks, created by honest miners, is:*

$$P_n(k) = \frac{p_H^n}{(n-1)!} \cdot \frac{e^{-\alpha_M n D_H} \cdot (\alpha_M n D_H)^k}{k!} \times$$

$$P(z) = \begin{cases} 1, & \text{if } p'_M \geq p'_H; \\ 1 - \sum_{k=0}^z P_z(k) \left(1 - \left(\frac{p'_M}{p'_H} \right)^{z-k} \right), & \text{otherwise,} \end{cases} \quad \times \sum_{i=0}^k \frac{(n-i+1)! \cdot C_k^i}{(\alpha n D_H)^i},$$

ПАЛИВНО-ЕНЕРГЕТИЧНИЙ СЕКТОР

Вперше **розроблено математичні моделі** атак на смартконтракти в енергетиці та на середовище їх функціонування – блокчейн.

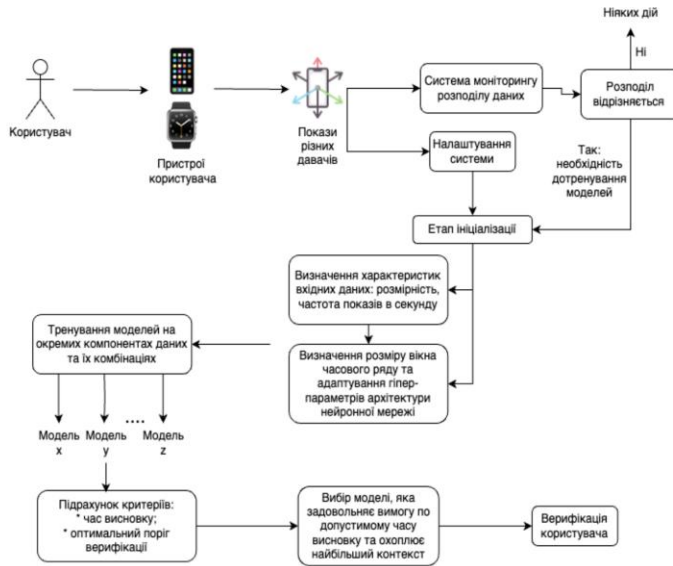
Удосконалено існуючі моделі атак на блокчейн (для різних протоколів консенсусу), внаслідок чого моделі стали більш реалістичними (враховано час затримки мережі, існування порожніх таймслотів, таймслотів з багатьма слотлідерами, нелінійність імовірності призначення слотлідера).

Отримано явні формули для оцінки імовірності успіху таких атак, які дозволяють вибрати таку кількість блоків підтвердження, після якої блок буде фіналізовано з імовірністю, як завгодно близькою до одиниці.



Моделі і методи теорії машинного навчання та штучного інтелекту для розв'язання проблем захисту критичної інфраструктури

Моделі біометричної верифікації та аутентифікації



Архітектура запропонованої СППР біометричної верифікації

Розроблена система верифікації дозволила зменшити ризик некоректної верифікації на 13%, порівняно з аналогічною системою без фрактальної розмірності даних.

Розроблено нові гібридні нейронні мережі на базі трансформера, які зменшують ризик некоректної верифікації в середньому на 11% та знижують час роботи системи в середньому на 31% у порівнянні з рекурентними автокодувальниками.

Розроблено та запропоновано нові гібридні архітектури автокодувальників на базі трансформерів для вирішення задачі верифікації з урахуванням фрактальної розмірності в даних, які можуть бути використані для захисту доступу до особливо критичних об'єктів в кібербезпеці та моніторингу медичних систем.

Верифікація користувача, як задача **бінарної класифікації** з відкритим другим класом (однокласова класифікація)

$$y_t = D(f(w_t^d))$$

$$f(w) = E(w) \rightarrow \min$$

- y_t — вихід системи верифікації в момент часу t ;
- D — вихід блоку прийняття рішення;
- f — вихід блоку виділення ознак та моделювання;
- w — вхідний сигнал з датчика.

Результатом роботи натренованої системи верифікації є віднесення користувача до класу "свій" або "чужий"

$$D = \sigma(E(w), \theta^*) = \begin{cases} 1 \text{ ("свій")} & \text{якщо } E(w) \leq \theta^* \\ 0 \text{ ("чужий")} & \text{в іншому випадку} \end{cases}$$

- $E(w)$ — вихід блоку виділення ознак та моделювання;
- θ^* — порогове значення для прийняття рішень щодо верифікації.

Model architecture	Average EER	Average FAR	Average FRR
Activity Triplet — read and sitting, write and sitting, map and sitting			
LSTM AE	1.26%	12.38%	0.06%
Transformer AE	1.61%	10.97%	0.14%
Activity Triplet – read and walking, write and walking, map and walking			
LSTM AE	9.10%	12.66%	9.51%
Transformer AE	6.47%	12.37%	4.81%

Model architecture	Training Time (s)	Inference Time (s)
LSTM AE (MSE loss)	90.67	43.32
Transformer-AE (MSE loss)	82.22	29.61
Difference	9.32%	31.65%

Метрика якості	Без ФРХ	З ФРХ	Різниця, %
Середній EER	0,16	0,14	-12,5
Середня AUC	0,89	0,91	+2,25
Середній FAR	0,029	0,026	-10,34
Середній FRR	0,15	0,138	-8

Автокодувальник

Метрика якості	Без ФРХ	З ФРХ	Різниця, %
Середній EER	0,15	0,13	-13,33
Середня AUC	0,90	0,92	+2,22
Середній FAR	0,021	0,02	-4,76
Середній FRR	0,174	0,149	-14,37

Автокодувальник на основі трансформера



**Моделі і методи
теорії машинного
навчання та
штучного
інтелекту для
розв'язання
проблем захисту
критичної
інфраструктури**

**Методи
напівкерowanego
навчання для задач
класифікації
фотографій
ракових
захворювань шкіри**

Метричні показники моделей для 5 % розмічених даних у навчальній вибірці

Назва методу напівкерowanego навчання	Accuracy	Precision (melanocytic nevi)	Precision (skin cancer)	Recall (melanocytic nevi)	Recall (skin cancer)	F1 (melanocytic nevi)	F1 (skin cancer)
CA ($\alpha = 0,25$)	0,778	0,797	0,727	0,884	0,580	0,838	0,645
CA ($\alpha = 0,5$)	0,777	0,819	0,690	0,843	0,653	0,831	0,671
CA ($\alpha = 1$)	0,778	0,808	0,709	0,865	0,615	0,835	0,658
VA	0,799	0,902	0,607	0,811	0,768	0,854	0,678
LN ($\alpha = 0,25$)	0,771	0,846	0,654	0,794	0,729	0,819	0,690
LN ($\alpha = 0,5$)	0,802	0,803	0,799	0,922	0,576	0,858	0,670
LN ($\alpha = 1$)	0,783	0,806	0,728	0,880	0,603	0,841	0,660
Etalon bad model	0,691	0,913	0,534	0,582	0,897	0,711	0,670
Etalon good model	0,847	0,852	0,796	0,903	0,712	0,883	0,756

Експерименти показали, що найефективнішим методом НН для малої кількості маркованих даних є Ladder Network з коефіцієнтом $\alpha = 0,5$ (приріст точності 11,1%, приріст F1 score 14,7% для класу 0 та 0% — для класу 1).

Найбільший приріст F1 score становив 2% для класу 1 для 5% маркованих даних, його показала модель LN при $\alpha = 0,25$.

Table 1. Fine Tuning Results

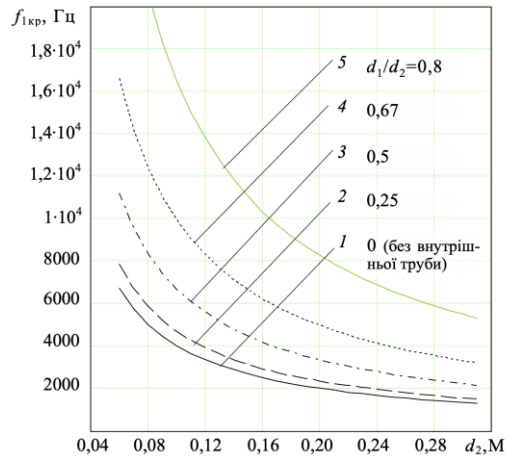
Model	Weights	Train Acc	Top-1 Acc	F1 AKEIC	F1 Df	F1 Mel
vit_1_32	imagenet1_v1	0.98	0.76	0.49	0.64	0.88
vit_1_16	imagenet1k_swag_linear_v1	0.85	0.8	0.44	0.75	0.9
VMamba-Г	vssmtiny_dp02_ckpt_epoch_258	0.95	0.8	0.6	0.76	0.9
VMamba-B	vssm_base_0229_ckpt_epoch_237	0.91	0.77	0.65	0.65	0.87

Порівняння моделей нейронних мереж архітектури “трансформер” та VMamba для виявлення раку шкіри по зображенню. Показано що VMamba має кращі F1 показники.



Моделі і методи теорії машинного навчання та штучного інтелекту для розв'язання проблем захисту критичної інфраструктури

Проблеми акустичного зондування глибоких свердловин



Залежність першої критичної частоти хвилевода типу «труба в трубі» від його геометричних розмірів

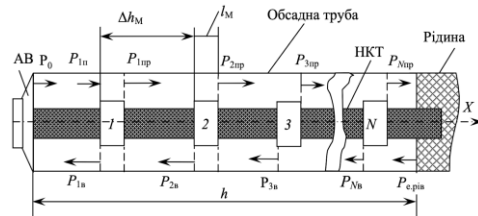
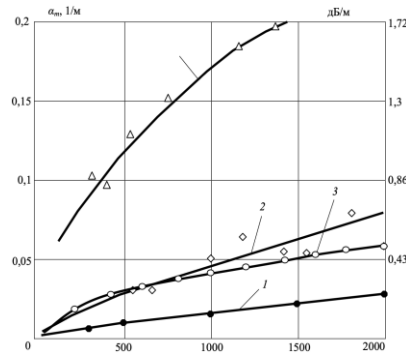
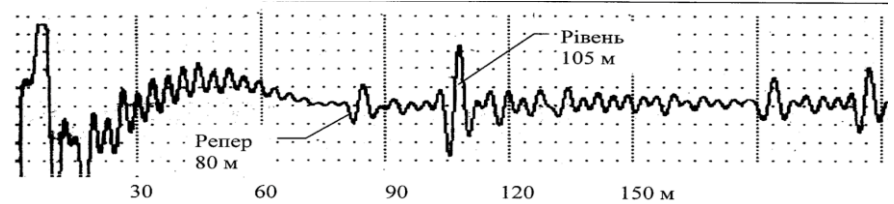


Схема відбиття та проходження хвиль у міжтрубному просторі нафтової свердловини



Згасання звуку в трубному хвилеводі, обумовлене пограничним тертям:
 1 — одинока труба 2b = 70 мм — теоретична крива;
 2 — одинока труба 2b = 70 мм — крива отримана експериментальним шляхом;
 3—4 — хвилевід типу «труба в трубі», 2b = 70 мм, 2a = 40 мм; 3 — теоретична крива; 4 — крива отримана експериментальним шляхом



Ехограма зондування артезійської свердловини (м. Київ) ехолотом «Скорпіон»

Уперше **розроблено і обґрунтовано** нову методику ехолокації у хвилеводах з використанням кількох нормальних хвиль, що суттєво підвищує точність за апіорі невідомої швидкості звуку.

Розроблено метод використання детермінованого складного сигналу з керованими параметрами, що дозволить шляхом оптимальної обробки виділити ехосигнали від з'єднувальних муфт і точніше визначити розподіл швидкості звуку по свердловині.

Розраховано акустичне поле у хвилеводі типу «труба в трубі». Обчислено першу критичну частоту.

Розроблені методи захищені патентами.

Запропоновані методики сприятимуть своєчасному виявленню дефектів та аварійних ситуацій, підвищуючи загальну безпеку експлуатації об'єктів.

До основних здобутків циклу робіт можна віднести, перш за все, наступні результати:

- ❖ розроблено стохастичні та ієрархічні динамічні моделі для планування оптимального розподілу ресурсів з метою захисту КІ від ризику терористичних атак та катастрофічних подій;
- ❖ створено методи оцінки ризиків на основі теорії катастроф та динамічних моделей, що враховують дефіцит даних;
- ❖ ведено новий клас полієдральних когерентних мір ризику для врахування ризику при пошуку оптимальних рішень в умовах невизначеності;
- ❖ запроваджено нові методи пошуку рівноважних децентралізованих рішень;
- ❖ розроблено ефективні алгоритми для варіаційних нерівностей, що застосовуються для оцінки екологічних ризиків, задач машинного навчання та ігрових моделей захисту КІ;
- ❖ розроблено нові методи оцінки стійкості немарковських блокових шифрів, оптимізації статистичних тестів для аналізу криптопримітивів та оцінки безпеки смарт-контрактів у децентралізованих ринках електроенергії;
- ❖ розроблено новий статистичний підхід до кількісної оцінки індивідуального безпекового ризику об'єктів критичної інфраструктури на основі оригінального непараметричного критерію однорідності вибірок та нових високоефективних алгоритмів моделювання та оптимізації масоперенесення в пористих середовищах для оцінки екологічних ризиків;
- ❖ розроблено алгоритми обробки ехосигналів акустичного зондування для покращення точності вимірювань, адаптивних моделей для ідентифікації невизначеностей, гібридних автокодувальників для біометричної верифікації підвищеної стійкості до змін вхідних даних.

Теоретичні засади моделювання проблем безпеки критичної інфраструктури покладені в основу вирішення фундаментальних та прикладних проблем, що досліджувались в рамках державних науково-технічних програм, на замовлення міністерств і відомств України, а також отримали підтримку міжнародних програм, фондів та організацій.

Практична значимість отриманих результатів підтверджується патентами, авторськими свідоцтвами, актами впровадження, свідоцтвами про реєстрацію авторських прав на твір, створенням сучасних інформаційних технологій світового рівня для дослідження складних процесів і систем, що функціонують в умовах ризику та невизначеностей. Одержані фундаментальні та практичні результати не поступаються, а у багатьох випадках перевищують рівень результатів відомих досліджень, що здійснювались провідними міжнародними і вітчизняними інституціями та фахівцями.

Світовий рівень роботи та її значимість підтверджені доповідями на багатьох міжнародних наукових конференціях, симпозіумах, семінарах, публікаціями у реферованих високореєтингових наукових виданнях, численними грантами від міжнародних наукових організацій для підтримки зазначених досліджень.

Загальна кількість посилань та індекс Хірша циклу робіт згідно наукометричних баз становить:

Web of Science - 1189, h-індекс - **15**; згідно **Scopus - 1773**, h-індекс - **20**; згідно **Google Scholar - 5516**, h-індекс – **30**.



РЕЗУЛЬТАТИ,

ВИСНОВКИ