НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

МЕТОДОЛОГІЯ СИНТЕЗУ МОДЕЛЕЙ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ УПРАВЛІННЯ ТА БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ЄВСЕЄВ С. П., ЗАКОВОРОТНИЙ О. Ю.,
МІЛОВ О. В., КУЧУК Г. А., ГАЛУЗА О. А.,
КОВАЛЬ М. В., ВОЙТКО О. В., ГРИЩУК Р. В.

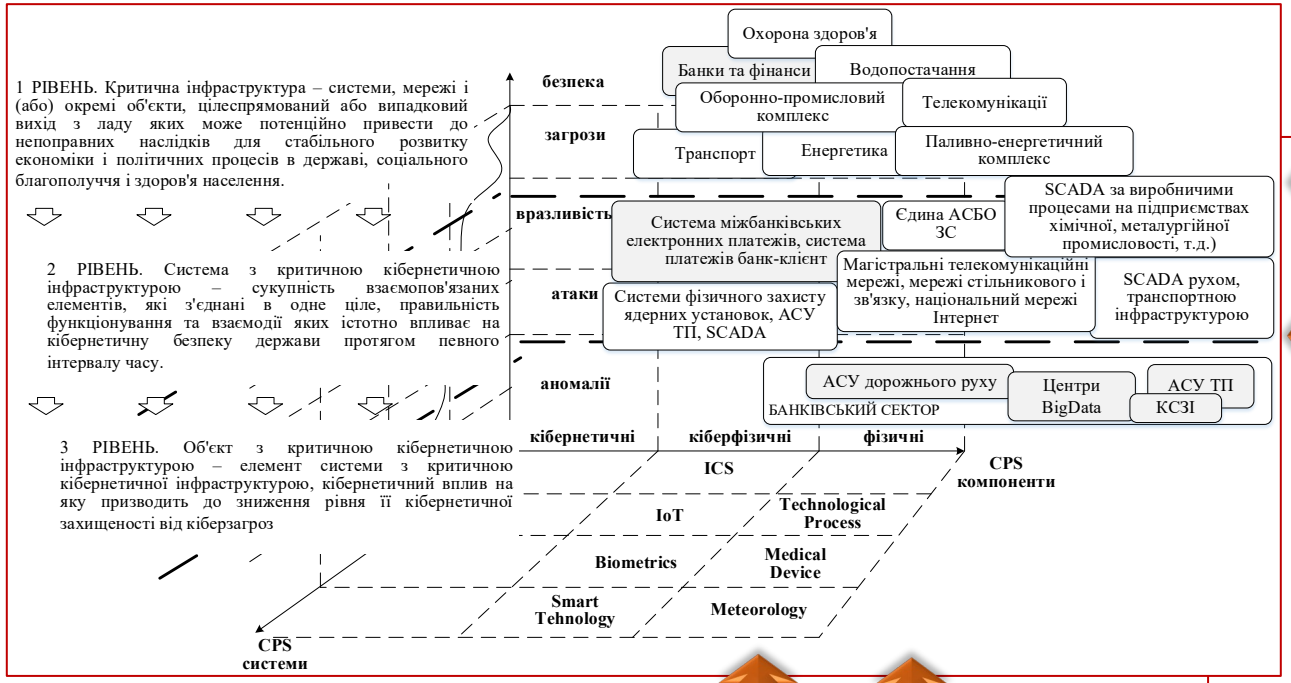
АКТУАЛНІСТЬ
МЕТА
КОНКУРЕНТО-СПРОМОЖНІСТЬ

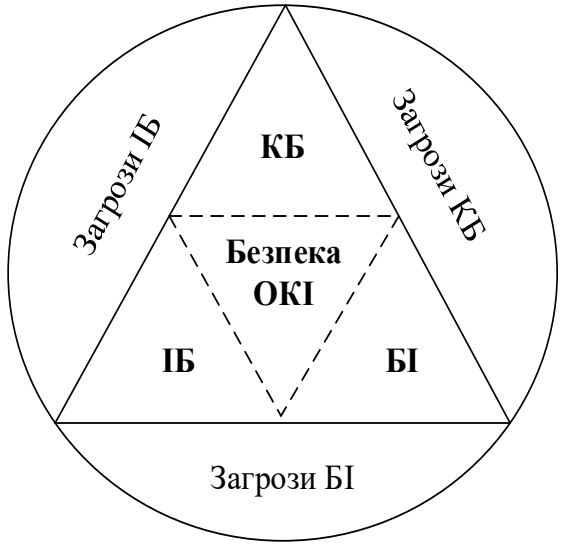
Актуальність роботи. Відсутність на сьогодні методології синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури обумовлено наявністю протиріччя, яке визначається тим, що з одного боку практика вимагає від теорії пошуку нових підходів до забезпечення безпеки інформаційних ресурсів об'єктів критичної інфраструктури в умовах зростання кількості цільових (змішаних) атак з ознаками синергії та гібридності (можливістю комплексування з методами соціальної інженерії), з іншого боку, в теорії відсутня цілісна науково обґрунтована методологія побудови на практиці системи безпеки інформації об'єктів критичної інфраструктури, що обумовлено недосконалістю механізмів забезпечення захищеності особливо у постквантовий період.

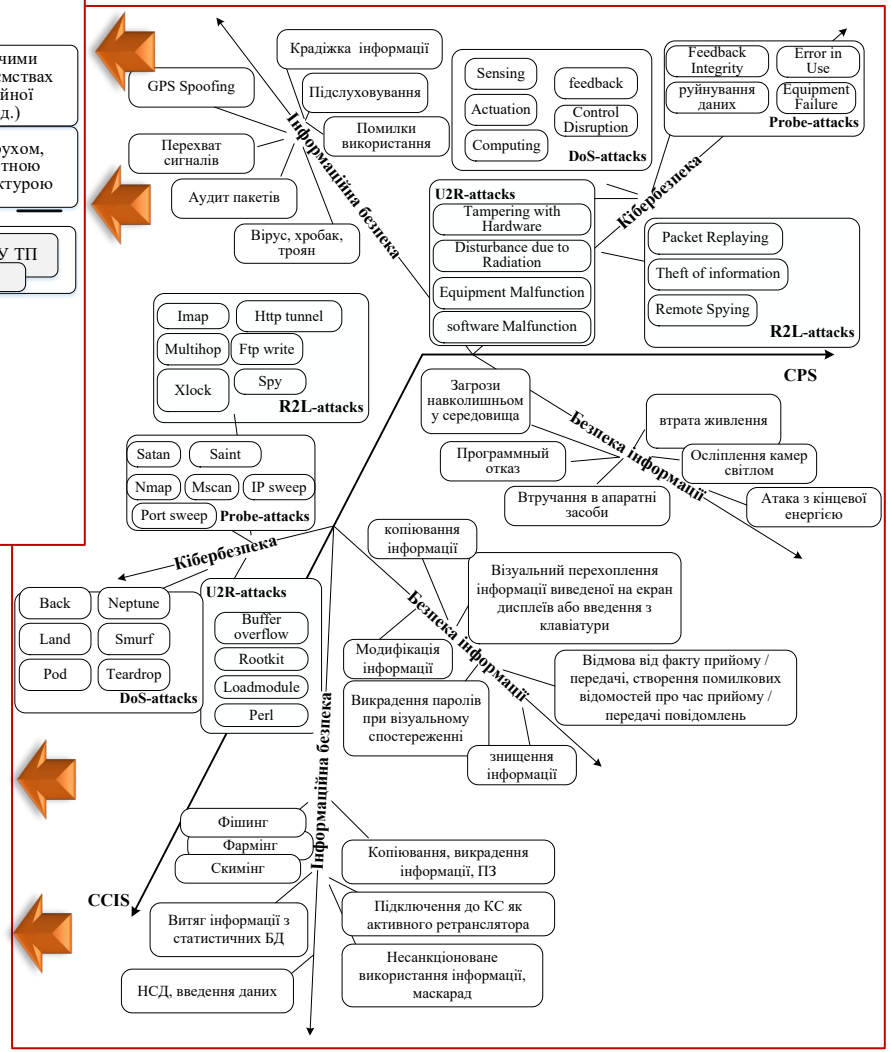
Конкурентоспроможність. Захищено 17 дисертацій, з них 7 – доктора наук, 6 – кандидата наук та 4 – доктора філософії. Кількість публікацій за роботою: 35 монографій, у т.ч. 4 у зарубіжних виданнях, 68 статей в журналах, включених до категорії "А" та 126 статей у журналах, включених до категорії "Б". Загальна кількість посилань на публікації авторів/h-індекс за роботою згідно з базами даних складає відповідно: Web of Science 16/17, Scopus 657/66, Google Scholar 2972/102. Отримано 5 патентів України на винахід, 55 патентів України на корисну модель, 2 свідоцтва авторського права на твір..

НТУ «ХПІ»

ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ БАГАТОКОНТУРНИХ СИСТЕМ БЕЗПЕКИ



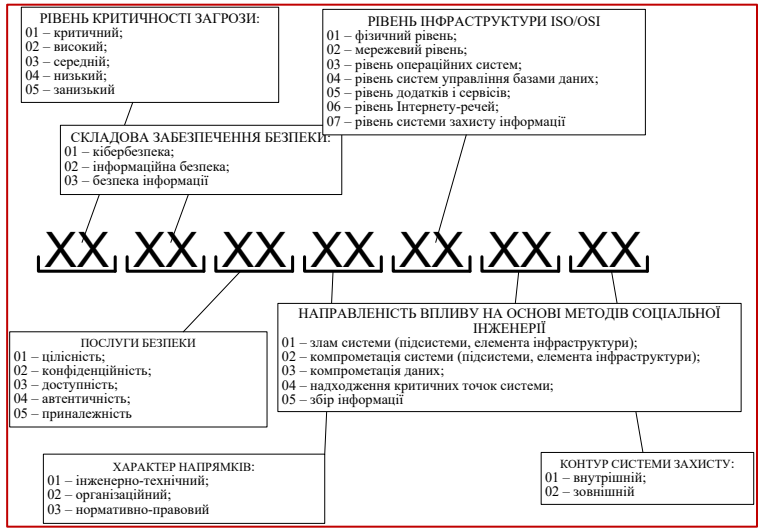


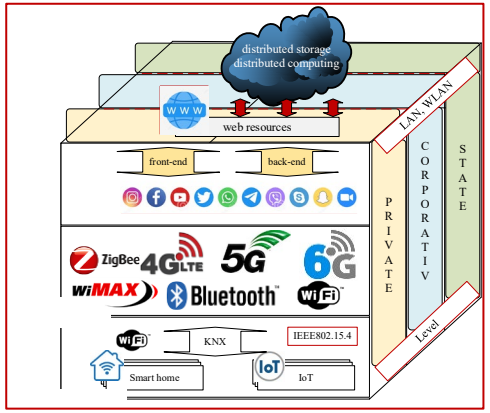


НТУ «ХПІ»

ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ БАГАТОКОНТУРНИХ СИСТЕМ БЕЗПЕКИ

Класифікатор загроз об'єктів критичної інфраструктури





Об'єкт критичної інфраструктури

Концепція багатоконтурних систем безпеки об'єктів критичної інфраструктури

загрози внутрішнього контуру з урахуванням гібридності та синергії загроз для 1-3 платформи

$$W^{SS\ ISL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{1\text{platform}}} = W^{SS\ ISL}_{synerg_{1\text{platform}}}{}^{C} \bigcap W^{SS\ ISL}_{synerg_{1\text{platform}}}{}^{I} \bigcap W^{SS\ ISL}_{synerg_{1\text{platform}}}{}^{A} \bigcap W^{SS\ ISL}_{synerg_{1\text{platform}}}{}^{Au} \bigcap W^{SS\ ISL}_{synerg_{1\text{platform}}}{}^{Inv},$$

$$W^{CS\ ISL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{2\text{platform}}} = W^{CS\ ISL}_{synerg_{2\text{platform}}}{}^{C} \bigcap W^{CS\ ISL}_{synerg_{2\text{platform}}}{}^{I} \bigcap W^{CS\ ISL}_{synerg_{2\text{platform}}}{}^{A} \bigcap W^{CS\ ISL}_{synerg_{2\text{platform}}}{}^{Au} \bigcap W^{CS\ ISL}_{synerg_{2\text{platform}}}{}^{Inv},$$

$$W^{CPS\ ISL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{3\text{platform}}} = W^{CPS\ ISL}_{synerg_{3\text{platform}}}{}^{C} \bigcap W^{CPS\ ISL}_{synerg_{3\text{platform}}}{}^{I} \bigcap W^{CPS\ ISL}_{synerg_{3\text{platform}}}{}^{A} \bigcap W^{CPS\ ISL}_{synerg_{3\text{platform}}}{}^{Au} \bigcap W^{CPS\ ISL}_{synerg_{3\text{platform}}}{}^{Inv},$$

загрози зовнішнього контуру з урахуванням гібридності та синергії загроз для 1-3 платформи

$$Q^{SCS\ ESL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{1\text{platform}}} = \left(Q^{SCS\ ESL}_{synerg_{1\text{platform}}}{}^{C} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SS\ ESL}_{synerg_{1\text{platform}}} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right)^{I} \cap \left(Q^{SCS\ ESL}_{synerg_{1\text{platform}}}{}^{A} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL}_{synerg_{1\text{platform}}}{}^{Au} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL}_{synerg_{1\text{platform}}}{}^{Inv} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right),$$

$$Q^{SCS\ ESL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{2\text{platform}}} = \left(Q^{SCS\ ESL}_{synerg_{2\text{platform}}}{}^{C} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL}_{synerg_{2\text{platform}}}{}^{I} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL}_{synerg_{2\text{platform}}}{}^{A} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL}_{synerg_{2\text{platform}}}{}^{Au} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL}_{synerg_{2\text{platform}}}{}^{Inv} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right),$$

$$Q^{SCS\ ESL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{3\text{platform}}} = \left(Q^{SCS\ ESL}_{synerg_{3\text{platform}}}{}^{C} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL}_{synerg_{3\text{platform}}}{}^{I} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL}_{synerg_{3\text{platform}}}{}^{A} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL}_{synerg_{3\text{platform}}}{}^{Au} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right) \cap \left(Q^{SCS\ ESL}_{synerg_{3\text{platform}}}{}^{Inv} \cup \sum_{i=1}^{5} S_i^{\text{sthreats}} \times \alpha_i\right),$$

$$Q^{SCS}_{ESL} = Q^{SCS\ ESL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{1\text{platform}}} \cup Q^{SCS\ ESL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{2\text{platform}}} \cup Q^{SCS\ ESL}_{\text{hybrid } C,I,A,Au,Af\ synerg_{3\text{platform}}}$$

Загальна оцінка загроз на многоконтурну систему захисту інформації

$$Q^{CPSS}_{\text{final}} = Q^{CPSS}_{ISL} \cup Q^{CPSS}_{ESL}.$$

Практична реалізація https://skl.sspu.sumy.ua/login

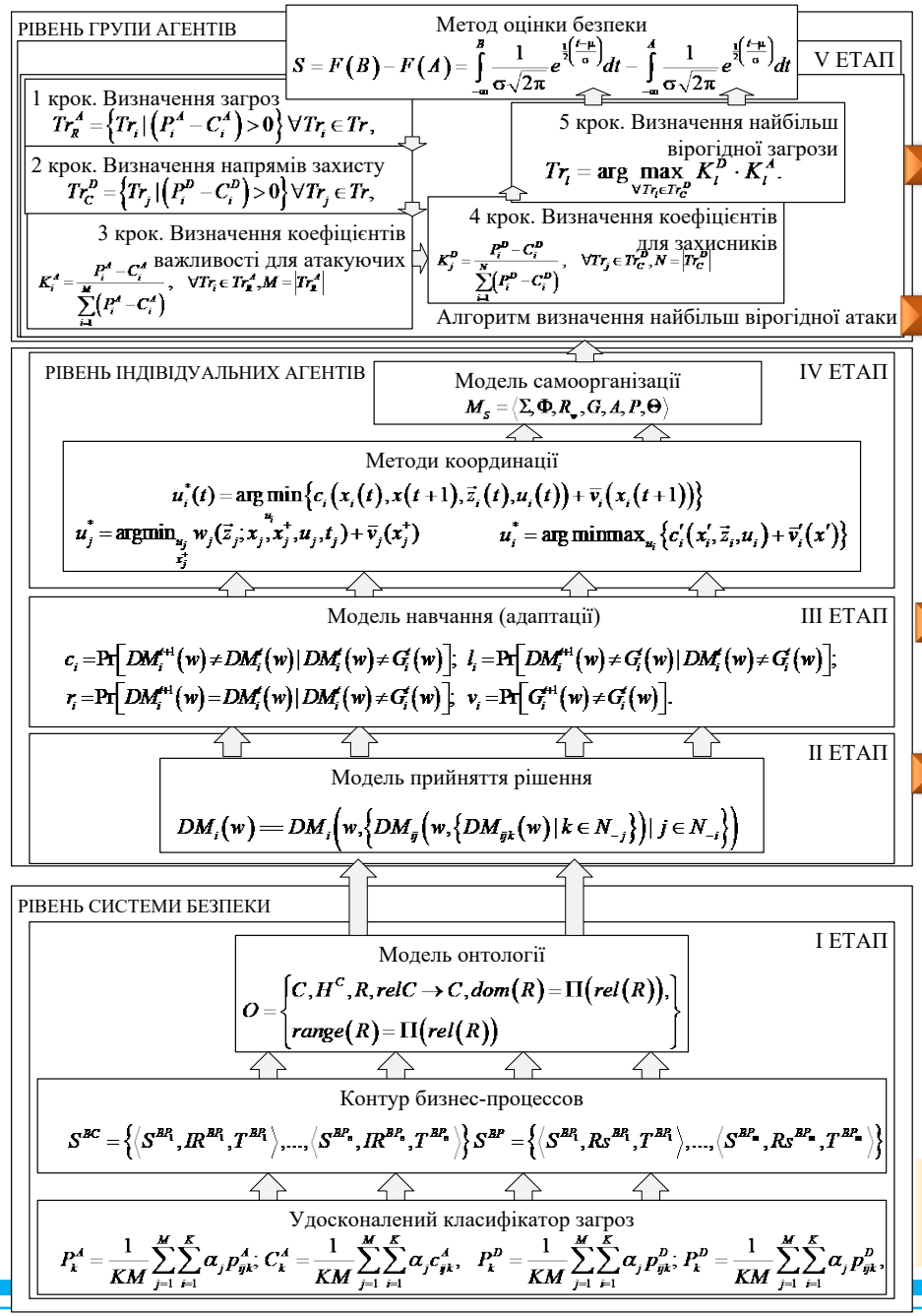
ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ БАГАТОКОНТУРНИХ СИСТЕМ БЕЗПЕКИ

Розроблено концепцію побудови синергетичної моделі загроз безпеки інформаційним ресурсам інтелектуальних систем управління та безпеки, базис якої становить трирівнева модель стратегічного управління безпекою об'єктів критичної інфраструктури. Розроблена на основі концепції модель шляхом комплексування складових інформаційної безпеки, кібербезпеки та безпеки інформації відкриває новий напрям у забезпеченні безпеки інформаційних ресурсів об'єктів критичної інфраструктури та враховує величину ризику на кожному рівні для дієвого контролю за виконанням інтелектуальними системами управління інформаційною безпекою критичної інфраструктури своїх функцій.

Удосконалено класифікатор загроз безпеці інформаційних ресурсів об'єктів критичної інфраструктури, який, на відміну від відомих, ґрунтується на синергетичній моделі загроз, що дозволяє класифікувати загрози за складовими безпеки, видами послуг та рівнями ієрархії об'єктів критичної інфраструктури, оцінювати синергію та гібридність загроз інформаційній безпеці, кібербезпеці, безпеці інформації, ймовірність їх впливу на безпеку інформаційних ресурсів. Для визначення об'єктивності експертної оцінки та автоматизації розроблений веб-застосунок (https://skl.sspu.sumy.ua/login), який дозволяє формувати експертну оцінку впливу загрози на послугу безпеки. Запропоновано визначити узгодженість димок експертів з різною мірою знань у галузі кібербезпеки та захисту інформації.

НТУ «ХПІ»

МОДЕЛЮВАННЯ ДІНАМІКИ ПОВЕДІНКИ ОБ'ЄКТІВ СИСТЕМ БЕЗПЕКИ



моделі оцінювання імовірностей здійснення загроз

1. Визначення загроз $Tr_R^A = \left\{ Tr_i \mid \left(P_i^A - C_i^A \right) > 0 \right\} \forall Tr_i \in Tr,$

2. Визначення напрямів захисту

$$Tr_C^D = \left\{ Tr_j \mid \left(P_i^D - C_i^D \right) > 0 \right\} \forall Tr_j \in Tr,$$

3. Визначення коефіцієнтів важливості для атакуючих

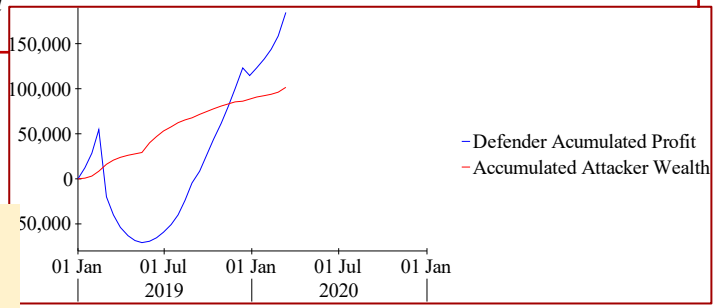
$$K_i^A = \frac{P_i^A - C_i^A}{\sum_{i=1}^{M} \left(P_i^A - C_i^A \right)}, \quad \forall Tr_i \in Tr_R^A, M = \left| Tr_R^A \right|$$

4. Визначення коефіцієнтів важливості для захисників

$$K_j^D = \frac{P_i^D - C_i^D}{\sum_{i=1}^{N} \left(P_i^D - C_i^D \right)}, \quad \forall Tr_j \in Tr_C^D, N = \left| Tr_C^D \right|$$

5. Визначення коефіцієнтів важливості для захисників

$$Tr_l = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A$$



Оцінка критичності зламу системи безпеки

МОДЕЛЮВАННЯ ДІНАМІКИ ПОВЕДІНКИ ОБ'ЄКТІВ СИСТЕМ БЕЗПЕКИ

Розроблено модель онтології поведінки агентів в умовах конфлікту, яка ґрунтується на базових поняттях процесів взаємодії агентів інтелектуальних систем управління та безпеки. Модель містить поняття та відносини, які відображають процеси взаємодії агентів протистояння, а не технічні параметри кіберконфлікту, що дозволяє обґрунтувати вибір моделей поведінки антагоністичних агентів в умовах впливу гібридних загроз на інформаційні ресурси інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури.

Розроблено рекурсивну модель рефлексивного агента, яка на відміну від чинних містить моделі поведінки сторони нападу, що дозволяє моделювати ймовірні дії протилежної сторони конфлікту і на визначеному горизонті прогнозу передбачати наслідки від прийнятих рішень стороною захисту.

Розроблено модель взаємодії агентів, яка дозволяє проводити імітаційне моделювання взаємодії агентів інтелектуальних систем безпеки під час кіберконфлікту, яка на відміну від чинних описує поведінку та параметри взаємодії всіх сторін кіберконфлікту, що дозволяє будувати ефективну стратегію мережевого захисту.

Вдосконалено модель самоорганізації інтелектуальних системи безпеки, яка відрізняється від чинних поєднанням в єдиній моделі складових прийняття рішень, рефлективності, адаптації та навчання, а її практична реалізація призводить до появи синергетичного ефекту під час захисту контуру бізнес-процесів об'єктів критичної інфраструктури

Запропонований підхід може застосовуватися для прогнозування можливої поведінки нападаючої сторони, обґрунтування вибору засобів протидії на системному рівні кіберзагрозам та розрахунку необхідної суми інвестицій у кібербезпеку з відповідним розподілом на напрямках та часу інвестування.

НТУ «ХПІ»

ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ БАГАТОКОНТУРНИХ СИСТЕМ БЕЗПЕКИ

$$A_1^{SCS} = \begin{cases} \frac{dN_1}{dt} = \left(\arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum_{i=1}^{Q} \begin{pmatrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix} \right) - \\ - \left(\sum_{i=1}^{M} \left(w_{SCSi}{}^C \cap w_{SCSi}{}^I \cap w_{SCSi}{}^A \cap w_{SCSi}{}^{Au} \cap w_{SCSi}{}^{Aff} \right) \chi_i^{SCS} \right) \tilde{N}_1 \times \\ \times \left(N_2 \times \left| W_{\text{hybrid } C,I,A,Au,Af \text{ synerg}} \right| \right); \\ \frac{dN_2}{dt} = - \left(\frac{1}{M} \sum_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \widetilde{N}_2 + \\ + \left(\frac{1}{KB} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\mu_{kg}^l \times w_{kg}^l \right) \right) \widetilde{N}_2 \widetilde{N}_1. \end{cases}$$

Модель безпеки з урахуванням обчислювальних можливостей та спрямованості цільових атак

$$A_1^{SCS} = \begin{cases} \frac{dN_1}{dt} = \left(\arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum_{i=1}^{Q} \begin{pmatrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix} \right) - \\ - \left(\sum_{i=1}^{M} \left(w_{SCSi}{}^C \cap w_{SCSi}{}^I \cap w_{SCSi}{}^A \cap w_{SCSi}{}^{Au} \cap w_{SCSi}{}^{Aff} \right) \chi_i^{SCS} \right) \tilde{N}_1 \times \\ \times \left(N_2 \times \left| W_{\text{hybrid } C,I,A,Au,Af \text{ synerg}} \right| \right); \\ \frac{dN_2}{dt} = - \left(\frac{1}{M} \sum_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \widetilde{N}_2 + \\ + \left(\frac{1}{KB} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\mu_{kg}^l \times w_{kg}^l \right) \right) \widetilde{N}_2 \widetilde{N}_1. \end{cases}$$

Модель з урахуванням можливої конкуренції зловмисників по відношенню до “жертви”

$$A_3^{SCS} = \begin{cases} \frac{dN_1}{dt} = \left(\arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum_{i=1}^{Q} \begin{pmatrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix} \right) - \\ - \left(\sum_{i=1}^{M} \left(w_{SCSi}{}^C \cap w_{SCSi}{}^I \cap w_{SCSi}{}^A \cap w_{SCSi}{}^{Au} \cap w_{SCSi}{}^{Aff} \right) \times \right. \\ \left. \times \chi_i^{SCS} \right) \times \\ \times \tilde{N}_1 \left(\widetilde{\sum_{j=1}^{w} N_2^w} \right); \\ \frac{dN_2}{dt} = - \left(\frac{1}{M} \sum_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \left(\widetilde{\sum_{j=1}^{w} N_2^w} \right) + \\ + \left(\frac{1}{KB} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\mu_{kg}^l \times w_{kg}^l \right) \right) \times \left(\widetilde{\sum_{j=1}^{w} N_2^w} \right) \widetilde{N}_1, \end{cases}$$

Модель з урахуванням можливості групування зловмисників/кібергруп з метою досягнення цілей кібератаки

$$A_4^{SCS} = \begin{cases} \frac{dN_1}{dt} = \left(\arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum_{i=1}^{Q} \begin{pmatrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix} \right) - \\ - \left(\sum_{i=1}^{M} \left(w_{SCSi}{}^C \cap w_{SCSi}{}^I \cap w_{SCSi}{}^A \cap w_{SCSi}{}^{Au} \cap w_{SCSi}{}^{Aff} \right) \times \right. \\ \left. \times \chi_i^{SCS} \right) \times \\ \times \tilde{N}_1 \left(\widetilde{\sum_{j=1}^{w} N_2^w} \right) - \varepsilon \widetilde{N_1}^2; \\ \frac{dN_2}{dt} = - \left(\frac{1}{M} \sum_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \left(\widetilde{\sum_{j=1}^{w} N_2^w} \right) + \\ + \left(\frac{1}{KB} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\mu_{kg}^l \times w_{kg}^l \right) \right) \times \left(\widetilde{\sum_{j=1}^{w} N_2^w} \right) \widetilde{N}_1 - \xi \widetilde{N_2}^2, \end{cases}$$

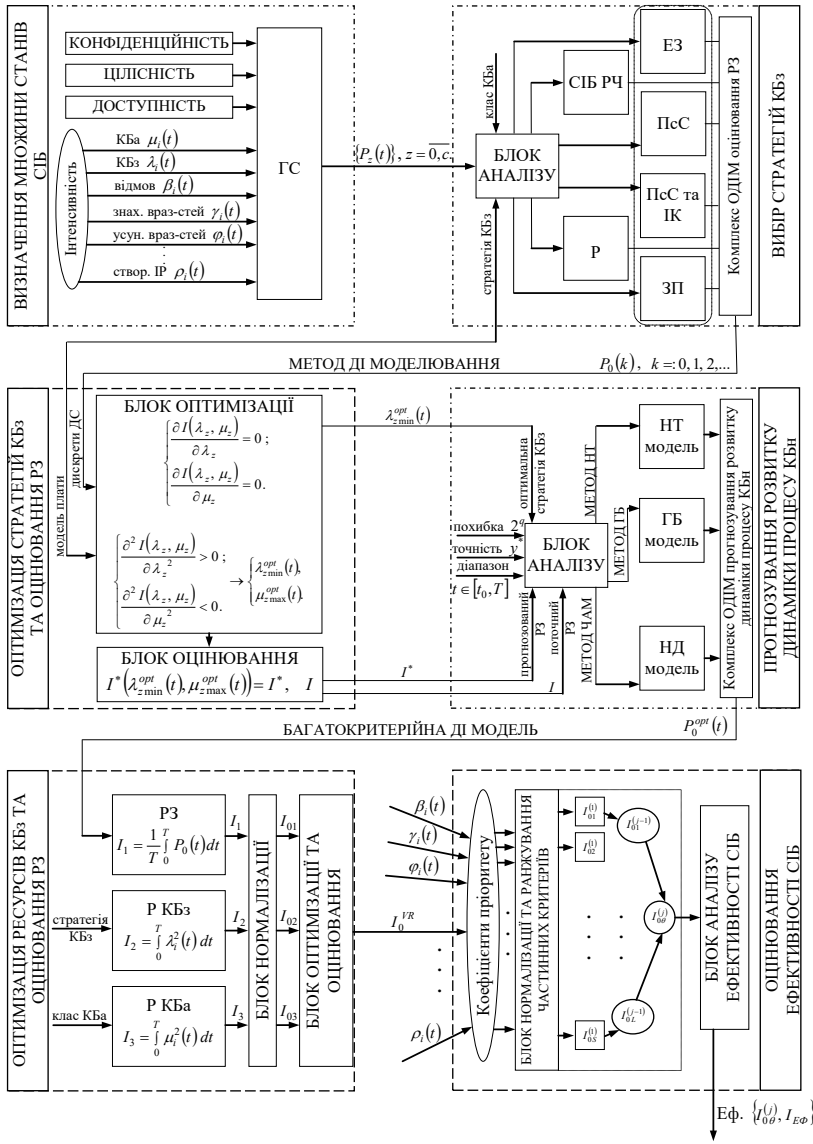
Модель з урахуванням взаємозв’язків між “видами жертв” та “видами хижаків”

ОСНОВАНІ НА МОДЕЛІ ЛОТКИ-ВОЛЬТЕРИ

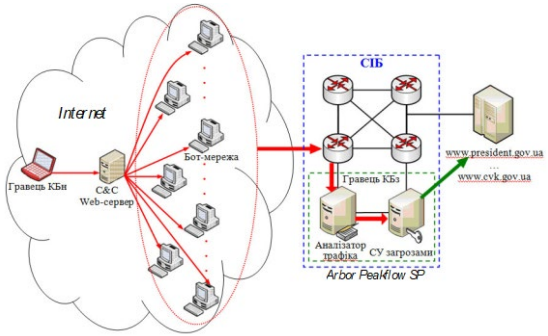
Розроблено динамічні моделі безпеки об’єктів критичної інфраструктури, які дозволяють враховувати обчислювальні можливості, конкурентні взаємодії між зловмисниками та їх “жертвами”, що дає можливість своєчасно визначити превентивні заходи протидії цільовим (змішаним) атакам.

НТУ «ХПІ»

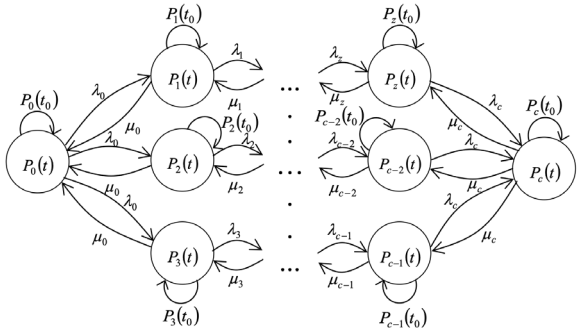
МОДЕЛЮВАННЯ ДІНАМІКИ ПОВЕДІНКИ ОБ'ЄКТІВ СИСТЕМ БЕЗПЕКИ



Розроблена методологія



Технологія кібернападу на веб-сайт Президента України



Узагальнена модель станів СІБ під час кібератаки

Крок 1. Визначення множини станів СІБ $\{P_z(t)\},\ z=\overline{0,c},\ t\in[t_0,T]$.

Крок 2. Побудова графової моделі

Крок 3. Складання системи диференціальних рівнянь Колмогорова-Чепмена

$$\frac{dP_z(t)}{dt}=f_z[P_0(t),P_1(t),\ldots,P_z(t),\lambda_0,\ldots,\lambda_z,\mu_0,\ldots,\mu_z],\ z=\overline{0,c}.$$

Крок 4. Задаються початкові умови, нормування та обмеження на ресурси гравців

$$\begin{cases}P_0(t_0)=1,\\ P_2(t_0)=\ldots=P_c(t_0)=0,\end{cases}\quad P_0(t_0)+\ldots+P_c(t_0)=1,\quad \begin{cases}0\le\mu_z\le\mu_{z\max},\\ 0\le\lambda_z\le\lambda_{z\max}.\end{cases}$$

Крок 5. Здійснення процедури моделювання

$$X(k)=\underline{x}(k)=\frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0}\quad x(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k X(k).$$

$$\begin{cases}P_0(k+1)=\frac{T}{k+1}\left[-3\lambda_0 P_0(k)+\mu_0\left(P_1(k)+P_2(k)+P_3(k)\right)\right];\\ P_1(k+1)=\frac{T}{k+1}\left[-(\mu_0+\lambda_1)P_1(k)+\ldots+\lambda_0 P_0(k)\right];\\ \vdots\\ P_c(k+1)=\frac{T}{k+1}\left[-3\mu_c P_0(k)+\lambda_c\left(P_z(k)+P_{c-2}(k)+P_{c-1}(k)\right)\right].\end{cases}\quad P_0(0)=[P_0(t_0)]=1\ \ P_0(1)=\ldots$$

Крок 6. Формування диференціально-ігрового базису

$$I=\sum_{k=0}^{k=\infty}\frac{P_0(k)}{k+1}\cdot\begin{cases}\frac{\partial I(\lambda_z,\mu_z)}{\partial\lambda_z}=0;\\ \frac{\partial I(\lambda_z,\mu_z)}{\partial\mu_z}=0.\end{cases}\rightarrow\begin{cases}\frac{\partial^2 I(\lambda_z,\mu_z)}{\partial\lambda_z^2}>0;\\ \frac{\partial^2 I(\lambda_z,\mu_z)}{\partial\mu_z^2}<0.\end{cases}\rightarrow\begin{cases}\lambda_{z\min}^{opt};\\ \mu_{z\max}^{opt}.\end{cases}\quad\Delta>0.\quad I^*.$$

$$P_0^{opt}(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k P_0^{opt}(k)\quad P_0(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k P_0(k).$$

Створено умови для побудови програмних та програмно-апаратних СІБ, інтегрованих до новостворюваних ІТ, стійких до кібератак прогнозованого класу

МОДЕЛЮВАННЯ ДІНАМІКИ ПОВЕДІНКИ ОБ'ЄКТІВ СИСТЕМ БЕЗПЕКИ

Вперше з системних позицій **обґрунтовано** належність системи управління об'єктів критичної інфраструктури до систем з критичною кіберінфраструктурою, що обумовлено їх функціонуванням під управлінням інформаційно-комунікаційних систем. Це дозволило розробити графову модель взаємодії систем управління об'єктів критичної інфраструктури, які є важливими для національної безпеки та оборони, а також економіки України. На основі розробленої моделі забезпечується завчасне виявлення таких об'єктів з поміж інших систем управління з обов'язковим оцінюванням їх рівня та категорії важливості для подальшого удосконалення необхідної інституційної бази, вироблення науково обґрунтованих пропозицій для виділення фінансових ресурсів на їх захист, запобігання виникненню ефектів ланцюгових реакцій, створення для цього необхідних організаційних безпекових структур з чіткою вертикаллю управління, оснащення їх необхідними апаратними та програмними засобами захисту державних інформаційних ресурсів.

Набула подальшого розвитку концепція побудови моделей розподілених систем інформаційної безпеки об'єктів критичної інфраструктури, яка на відміну від відомих ґрунтується на моделях напівмарковських процесів, що дозволяють в реальному масштабі часу відстежувати динаміку протікання процесів кібернападу у ході кіберконфлікту в системі інформаційної безпеки об'єкта під час кібератаки та, на основі накопичених знань, прогнозувати такі безпекові інциденти для визначеного класу систем управління та безпеки у майбутньому. Розроблені на основі концепції диференціально-ігрові моделі дозволяють виробляти відповідні політики безпеки для нового класу систем захисту – інтелектуальних систем безпеки об'єктів критичної інфраструктури

НТУ «ХПІ»

МОДЕЛЮВАННЯ ДІНАМІКИ ПОВЕДІНКИ ОБ'ЄКТІВ СИСТЕМ БЕЗПЕКИ

$$
\begin{cases}
P_0(k+1)=\frac{T}{k+1}\left[-\lambda P_0(k)+\frac{1}{3}\mu P_3(k)+\frac{1}{3}\mu T P_4(k-1)+\right.\\
\left.+\frac{1}{3}\sum_{l=0}^{k}\frac{(\mu T)^{k-l}}{(k-l)!}P_5(l)\right];\\
P_1(k+1)=\frac{T}{k+1}\left[-\lambda T P_1(k-1)+\frac{1}{3}\mu P_3(k)+\frac{1}{3}\mu T P_4(k-1)+\right.\\
\left.+\frac{1}{3}\sum_{l=0}^{k}\frac{(\mu T)^{k-l}}{(k-l)!}P_5(l)\right];\\
P_2(k+1)=\frac{T}{k+1}\left[-\sum_{l=0}^{k}\frac{(\lambda T)^{k-l}}{(k-l)!}P_2(l)+\frac{1}{3}\mu P_3(k)+\right.\\
\left.+\frac{1}{3}\mu T P_4(k-1)+\frac{1}{3}\sum_{l=0}^{k}\frac{(\mu T)^{k-l}}{(k-l)!}P_5(l)\right];\\
P_3(k+1)=\frac{T}{k+1}\left[-\mu P_3(k)+\lambda P_0(k)+\frac{1}{2}\lambda T P_1(k-1)+\right.\\
\left.+\frac{1}{2}\sum_{l=0}^{k}\frac{(\lambda T)^{k-l}}{(k-l)!}P_2(l)\right];\\
P_4(k+1)=\frac{T}{k+1}\left[-\mu T P_4(k-1)+\frac{1}{2}\lambda T P_1(k-1)\right];\\
P_5(k+1)=\frac{T}{k+1}\left[-\sum_{l=0}^{k}\frac{(\mu T)^{k-l}}{(k-l)!}P_5(l)+\frac{1}{2}\sum_{l=0}^{k}\frac{(\lambda T)^{k-l}}{(k-l)!}P_2(l)\right],
\end{cases}
$$

Диференціально-ігрова модель розподіленої системи інформаційної безпеки

$$
P_0^{NT}(t)=\frac{\lambda}{\lambda+\mu}e^{-(\lambda+\mu)t}+\frac{\mu}{\lambda+\mu}
$$

Диференціально-ігрова нетейлорівська модель

$$
E_1=\sum_{i=1}^{\psi}\frac{1}{v_i L_\psi}\sum_{m=1}^{S_1}\varepsilon_m\left[a_m-\sum_{j=1}^{S_2}\lambda_{mj}\lambda_{ij}\right]=
$$

$$
=\frac{\psi}{L_\psi}\varepsilon_m\left[\sum_{j=1}^{S_2}\sum_{m=1}^{S_1}\beta_{jm}a_m\lambda_{mj}\right]-\sum_{i=1}^{\psi}\frac{1}{L_\psi}\sum_{m=1}^{S_1}\varepsilon_m\sum_{j=1}^{S_2}\lambda_{mj}\lambda_{ij}\geq
$$

$$
\geq\sum_{m=1}^{S_1}\varepsilon_m\sum_{j=1}^{S_2}\left[\psi(j)\sum_{m=1}^{S_1}\beta_{jm}a_m\lambda_{mj}\right]\frac{1}{L_{\psi(j)}}-\sum_{m=1}^{S_1}\varepsilon_m\sum_{j=1}^{S_2}\frac{\lambda_{mj}d_j}{L_{\psi(j)}}=
$$

$$
=\sum_{m=1}^{S_1}\sum_{j=1}^{S_2}\frac{\varepsilon_m\lambda_{mj}}{L_{\psi(j)}}\left[\psi(j)\sum_{m=1}^{S_1}\beta_{jm}a_m-d_j\right]=I^*
$$

$$
E_2=v_i\sum_{m=1}^{S_1}\varepsilon_m\left\{\mu_{im}-\sum_{j=1}^{S_2}\lambda_{mj}\left[\beta_{jm}\left(a_m-\frac{I_m}{v_i\varepsilon_m}\right)\right]\right\}\leq
$$

$$
\leq v_i\left\{\sum_{m=1}^{S_1}\varepsilon_m\left[a_m-\sum_{j=1}^{S_2}\sum_{m=1}^{S_1}\beta_{jm}a_m\lambda_{mj}+\sum_{j=1}^{S_2}\sum_{m=1}^{S_1}\beta_{jm}\frac{I_m}{v_i\varepsilon_m}\lambda_{mj}\right]\right\}=
$$

$$
=v_i\left\{\sum_{m=1}^{S_1}\varepsilon_m a_m-\left[\sum_{m=1}^{S_1}\varepsilon_m a_m+\sum_{m=1}^{S_1}\frac{I_m}{v_i}\right]\right\}=I
$$

Моделі оцінки оптимальності стратегій гравців в інформаційному конфлікті

$$
I(\lambda,\mu)=\sum_{i=1}^{n}v_i\max\left\{0,\sum_{m=1}^{S_1}\varepsilon_m\left(\mu_{im}-\sum_{j=1}^{S_2}\lambda_{mj}\lambda_{ij}\right)\right\}
$$

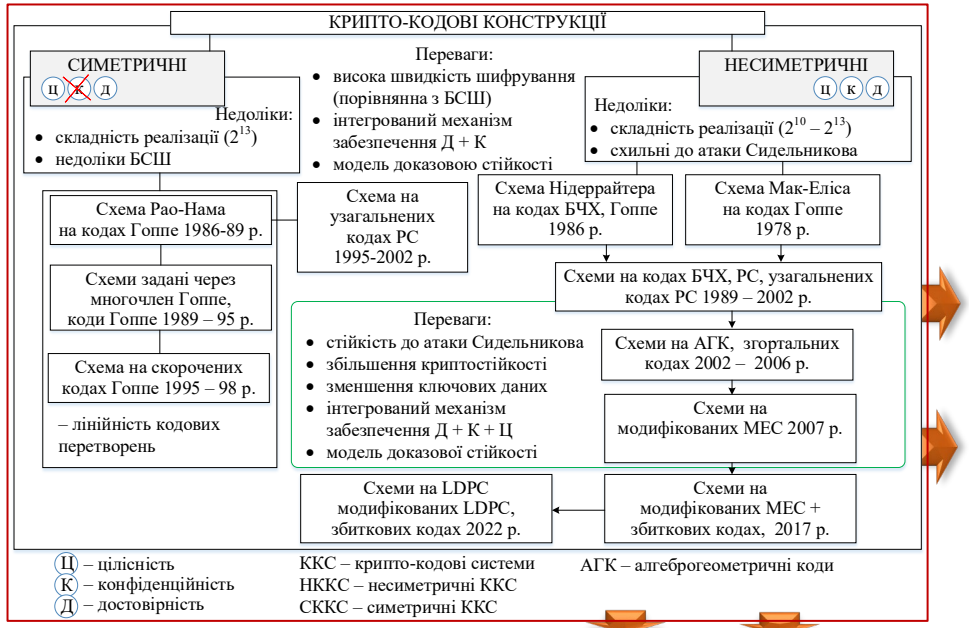
Оцінка сумарних втрат цілісності, доступності та конфіденційності

МОДЕЛЮВАННЯ ДІНАМІКИ ПОВЕДІНКИ ОБ’ЄКТІВ СИСТЕМ БЕЗПЕКИ

Вперше синтезовано комплекс багатокритерійних диференціально-ігрових моделей процесів кібернападу на державні інформаційні ресурси об’єктів критичної інфраструктури, який базується на нелінійній схемі компромісів та диференціальних перетвореннях, що дозволяє регуляризувати вихідну некоректну задачу моделювання з конфліктуючими частинними критеріями та зводити проблему динамічної векторної оптимізації до рішення системи лінійних алгебричних рівнянь відносно вхідних параметрів розроблюваних моделей. Застосування синтезованого комплексу моделей дозволяє отримувати кількісні та якісні оцінки ефективності систем інформаційної безпеки, відкриває шлях до подальшого розвитку науково обґрунтованого підходу щодо вибору показників ефективності за обраними частинним критеріями, а також дозволяє встановлювати емерджентні властивості комплексних систем захисту інформації об’єктів критичної інфраструктури.

НТУ «ХПІ»

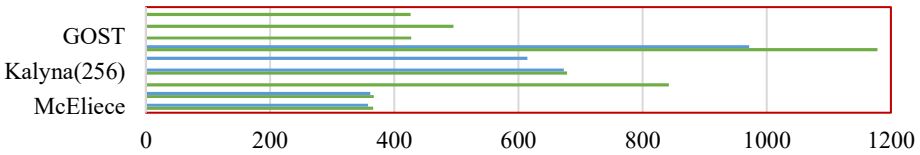
МЕХАНІЗМИ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ПОСЛУГ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ



Властивість	Укорочені *LDPC*-коди	Подовжені *LDPC*-коди
(N, k) параметри коду	$N = 2\sqrt{q} + q + 1 - x, \quad k \langle N$	$N = 2\sqrt{q} + q + 1 - x + x_1, \quad k \langle N$
Довжина відкритого тексту	$l_I = l_z^e + l_z^f$	$l_I = 1/2k \times m + l_z^e + l_z^f$
Довжина кодограми (в бітах)	$l_S = \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m;$	$l_S = \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m.$
Довжина відкритого ключа (в бітах)	$l_K = 1/2k \times \left(2\sqrt{q} + q + 1 - 1/2k\right.$	$l_K = 1/2k \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m.$
Довжина закритого ключа (в бітах)	$l_{K+} = 1/2k \left\lceil \log_2\left(2\sqrt{q} + q + 1\right)\right\rceil$	$l_{K+} = \left(1/2k - 1/2k\right) \left\lceil \log_2\left(2\sqrt{q} + q + 1\right)\right.$
Складність формування кодограми для систематичного кодування	$O_K = (r+1) \times \left(2\sqrt{q} + q + 1 - 1/2k\right) + +O\left(\frac{1 - K_C^u}{K_f} \times L\right);$	$O_K = (r+1) \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) + +O\left(\frac{1 - K_C^u}{K_f} \times L\right);$
Складність формування кодограми для несистематичного кодування	$O_K = O_K = (k+1) \times (k+1) \times \times \left(2\sqrt{q} + q + 1 - 1/2k\right) + +O\left(\frac{1 - K_C^u}{K_e} \times L\right);$	$O_K = (k+1) \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) + +O\left(\frac{1 - K_C^u}{K_f} \times L\right).$
Складність разкодування кодограми	$O_{SK} = 2 \times \left(2\sqrt{q} + q + 1 - 1/2k\right)^2 + 1/2k^2 + +4t^2 + \left(t^2 + t - 2\right)^2 / 4 + O\left(\frac{\alpha - z \times \log k}{\lvert K_z^c \times L \rvert}\right);$	$O_{SK} = 2 \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right)^2 + +k^2 + 4t^2 + \left(t^2 + t - 2\right)^2 / 4 + O\left(\frac{\alpha - z \times \log k}{\lvert K_z^c \times L \rvert}\right).$
Складність процесу декодування	$O_{K+} = N_{покр} \times \left(2\sqrt{q} + q + 1 - 1/2k\right) \times r + +N_{F\,або}(N_K),$	$O_{K+} = N_{покр} \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times \times r + N_F$ або $(N_K).$

Властивість	Укорочені *МЕС*	Подовжені *МЕС*
(n, k, d) параметри коду, який побудований через відображення виду $\varphi: X \to P^{k-1}$	$n = 2\sqrt{q} + q + 1 - x,$ $k \geq \alpha - x,\ d \geq n - \alpha,$ $\alpha = 3 \times degF,$ $k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1,$ $k \geq \alpha - x + x_1,\ d \geq n - \alpha,$ $\alpha = 3 \times degF$
n, k, d) параметри коду, який побудований через відображення виду $\varphi: X \to P^{r-1}$	$n = 2\sqrt{q} + q + 1 - x,$ $k \geq n - \alpha,\ d \geq \alpha,$ $\alpha = 3 \times degF,\ k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1,$ $k \geq n - \alpha,\ d \geq \alpha,$ $\alpha = 3 \times degF$

Властивість	Укорочені *МЕС*	Подовжені *МЕС*
розмірність секретного ключа	$l_{K+} = x \times \left\lceil \log_2\left(2\sqrt{q} + q + 1\right)\right\rceil$	$l_{K+} = (x - x_1) \times \log_2\left(2\sqrt{q} + q + 1\right)$
розмірність інформаційного вектора	$l_I = (\alpha - x) \times m$	$l_I = (\alpha - x + x_1) \times m$
розмірність криптограми	$l_S = \left(2\sqrt{q} + q + 1 - x\right) \times m$	$l_S = \left(2\sqrt{q} + q + 1 - x + x_1\right) \times m$
відносна швидкість передачі	$R = (\alpha - x) / \left(2\sqrt{q} + q + 1 - x\right)$	$R = (\alpha - x + x_1) / \left(2\sqrt{q} + q + 1 - x + x_1\right)$

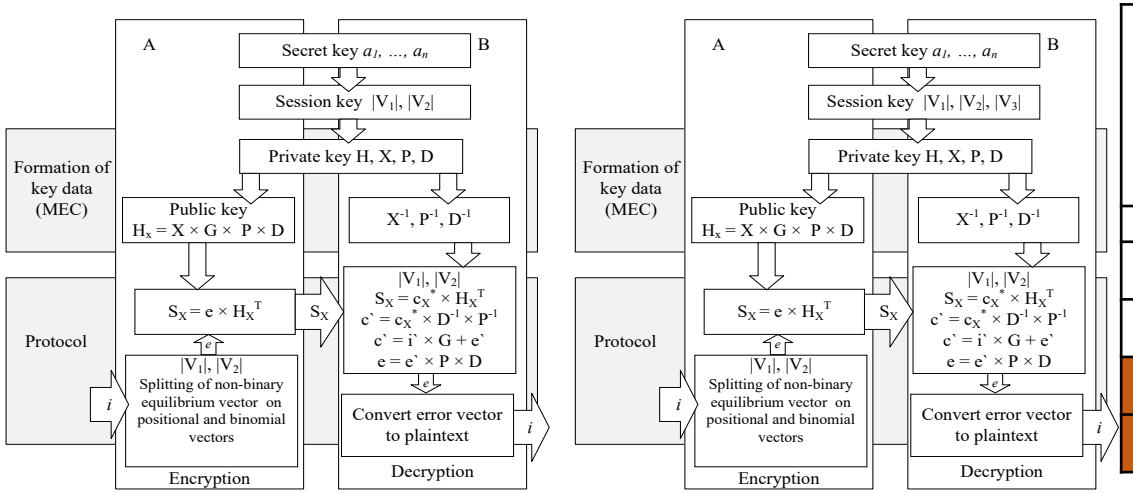


	McEliece	Niederreiter	Kalyna(128)	Kalyna(256)	Kalyna(512)	AES	GOST	BelT	Kuznyechik
256 bit	357,534	361,239		673,174	614,239	971,725			
128 bit	365,551	366,614	842,061	678,096		1177,95	427,362	495,39	425,908

Оцінка швидкодії криптоперетворень

НТУ «ХПІ»

МЕХАНІЗМИ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ПОСЛУГ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ



Криптосистеми	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей	Кількість тестів, в яких тестування пройшли менше 96% послідовностей
CCC McElice	149 (78,83%)	189 (100%)	0 (0%)
CCC McElice на укор. МЕС	151 (79,89%)	189 (100%)	0 (0%)
CCC McElice подовжю МЕС	152 (80,42%)	189 (100%)	0 (0%)
НССС на подовж. МЕС	153 (80,95%)	189 (100%)	0 (0%)
НССС на укор. МЕС	155 (82 %)	189 (100%)	0 (0%)

Результати дослідження статистичної безпеки

Криптосистеми	*GF* (q^m)						
	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
ССС Мак-Еліса на укорочених МЕС	8293075	10007947	**17787431**	28595014	44079433	61974253	79554764
ССС Мак-Еліса на подовжених МЕС	8506422	11156138	**18561228**	33210708	48297112	65171690	84051337
НССС подовж.МЕС	**5612316**	7900315	14892945	25565274	42279183	58963778	76564173
НССС укор. МЕС	**5942627**	7905257	14682411	25595014	42116327	58468143	75474764

Залежність швидкості програмної реалізації від потужності поля

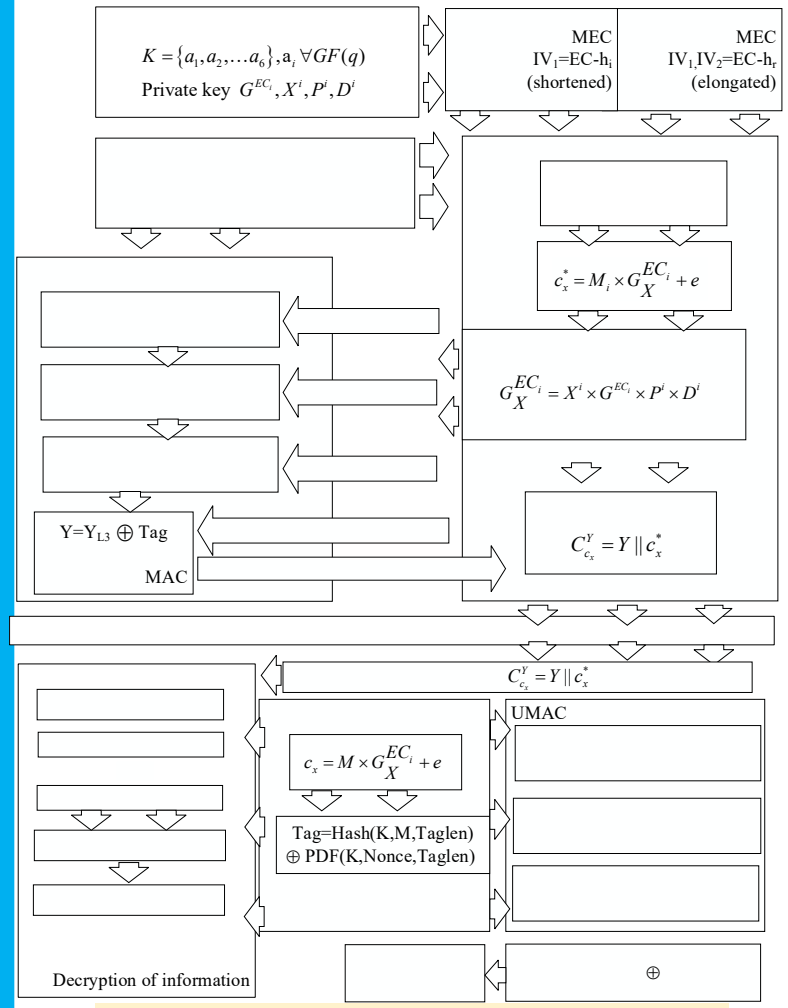
$lg(l_s)$	*R*							
	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)	0.5(udh)	0.75(udh)	0.5(ukh)	0.75(ukh)
1	15.6	18.23	19.12	19.82	7.21	9.17	12.54	14.56
2	32.47	35.67	38.63	39.18	21.46	23.72	27.48	29.82
3	43.75	51.61	56.88	58.03	31.68	33.83	37.38	38.43
4	59.43	72.81	78.92	80.52	**41.72**	**42.27**	**47.48**	**58.23**
5	68.26	87.32	94.91	104.56	56.63	58.91	62.86	66.53
6	**101.72**	**112.46**	**120.83**	**128.79**	72.32	74.79	89.5	97.71

Зведена діаграма складності зламу і складності кодування для різних швидкостей МЕС

Практична реалізація https://www.calltools.ua/en/

НТУ «ХПІ»

МЕХАНІЗМИ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ПОСЛУГ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ



Удосконалений протокол SSL/TLS на ССС

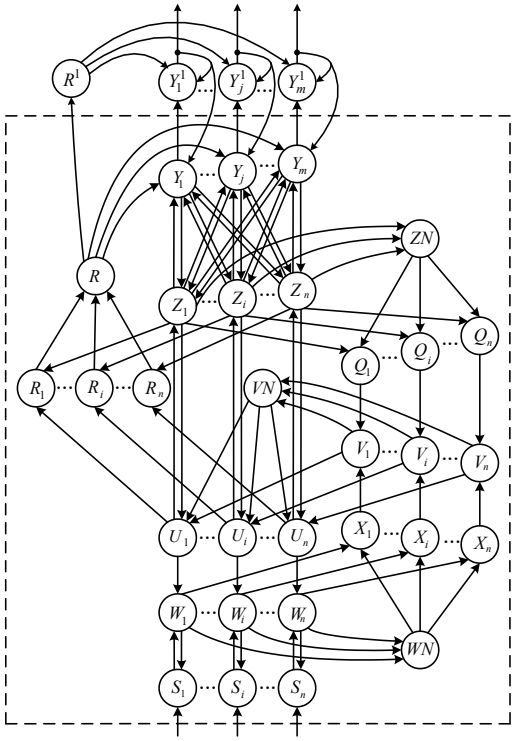
Розроблені та **запатентовані** моделі крипто-кодових конструкцій Мак-Еліса та Нідеррайтера на еліптичних (модифікованих еліптичних) кодах та гібридних крипто-кодових конструкціях зі збитковими кодами, що дозволяє підвищити рівень інформаційної прихованості та достовірності інформаційних ресурсів об'єктів критичної інфраструктури в умовах впливу гібридних загроз на об'єкти критичної інфраструктури в постквантовий криптоперіод

Набула подальшого розвитку модель забезпечення автентичності інформаційних ресурсів, яка ґрунтується на удосконаленому протоколі SSL/TLS на крипто-кодових конструкціях Мак-Еліса та Нідеррайтера, що дозволяє реалізувати послуги безпеки на об'єктах критичної інфраструктури в умовах появи повномасштабного квантового комп'ютера

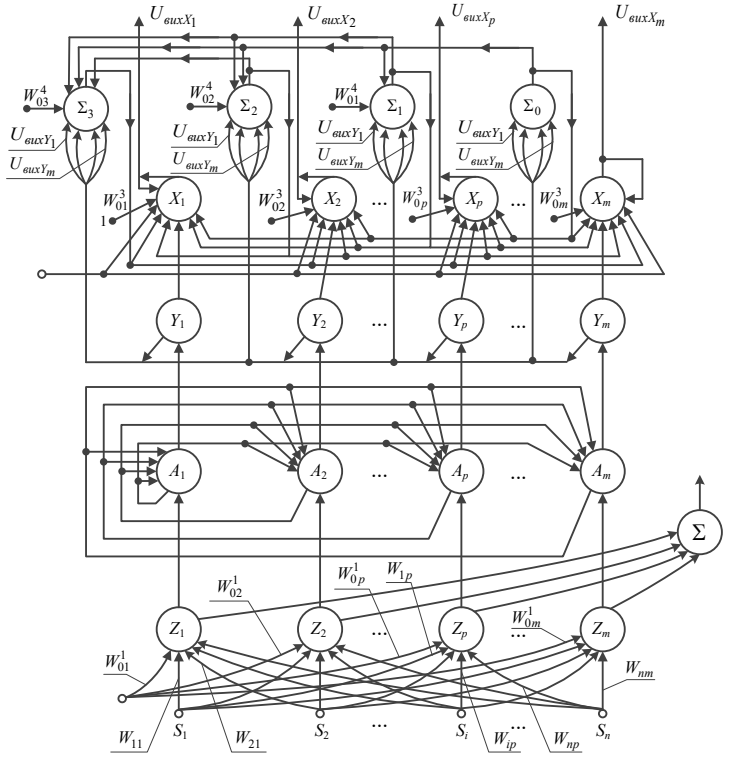
Основною відмінністю від відомих підходів є за збереження рівня пропускних можливостей бездротового каналу інтегровано забезпечити необхідний рівень захищеності (криптостійкості) каналу (криптостійкість на основі постквантових алгоритмів на рівні 10^{25}–10^{35} групових операцій), достовірності ($P_{пом}$ не нижче 10^{-9}–10^{-12}), а використання збиткових кодів і подальше зменшення потужності поля Галуа призводить до значного зменшення складності формування (≈ в 12 разів) і розкодування криптограми (≈в 20 разів).

НТУ «ХПІ»

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ КЕРУВАННЯ ОБ'ЄКТАМИ ТА БАЗИ ЗНАНЬ НА ОСНОВІ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ



Архітектури нових нейронних мереж адаптивної резонансної теорії, що визначають декілька рівноцінних рішень.

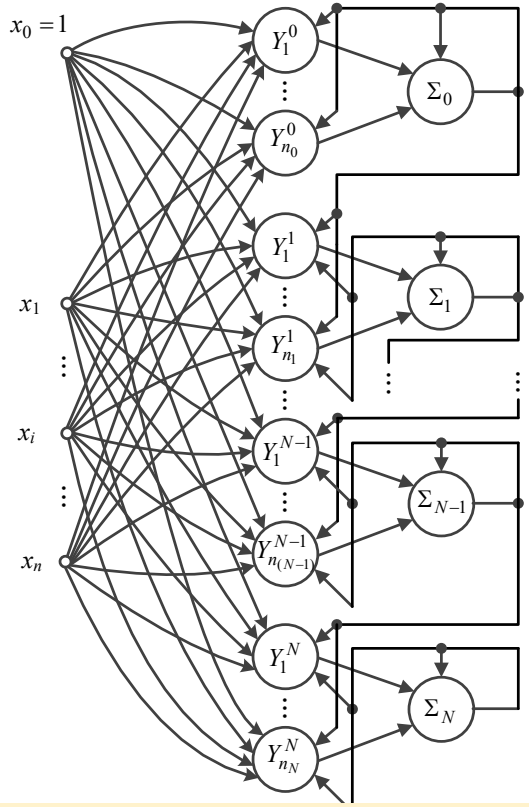


Архітектури нейронних мереж Хеммінга, що донавчатися та визначають декілька рівноцінних рішень.

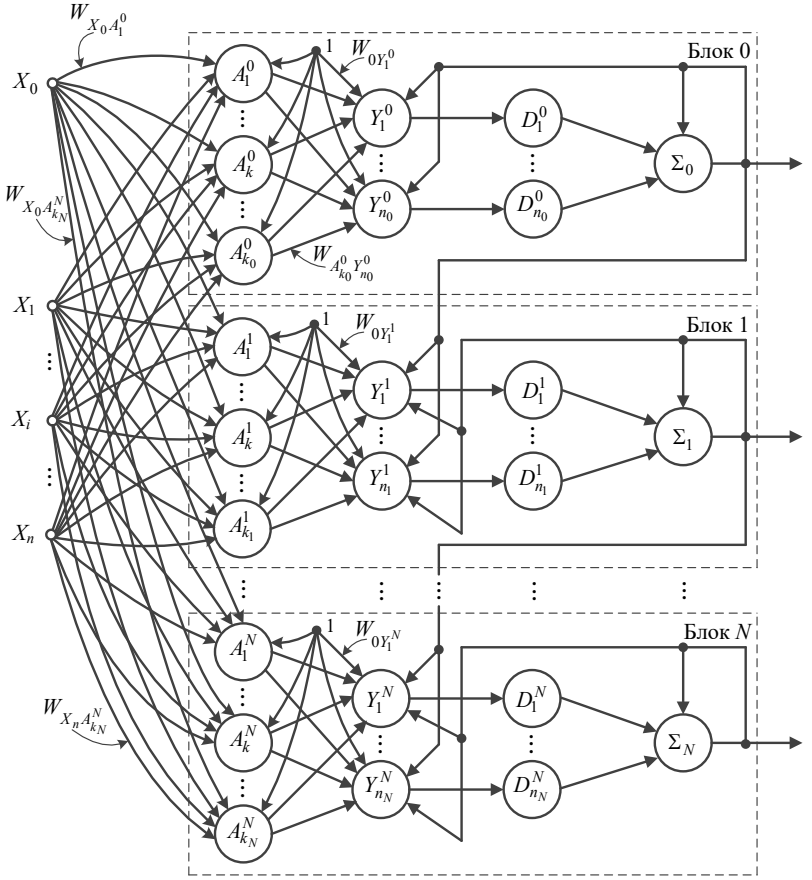
Розроблені інтелектуальні бази даних і знань, на основі штучних нейронних мережі, здатні розпізнавати нову інформацію, донавчатися в процесі функціонування та визначати декілька рівноцінних рішень, що дозволяє виконати перевірку працездатності запатентованих алгоритмів та створювати на їх основі нові інтелектуальні системи управління та безпеки об'єктів критичної інфраструктури, які можуть донавчатися в процесі експлуатації й визначати декілька рівноцінних рішень.

НТУ «ХПІ»

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ КЕРУВАННЯ ОБ’ЄКТАМИ ТА БАЗИ ЗНАНЬ НА ОСНОВІ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ



Архітектура нейронної мережі Хебба, що донавчається

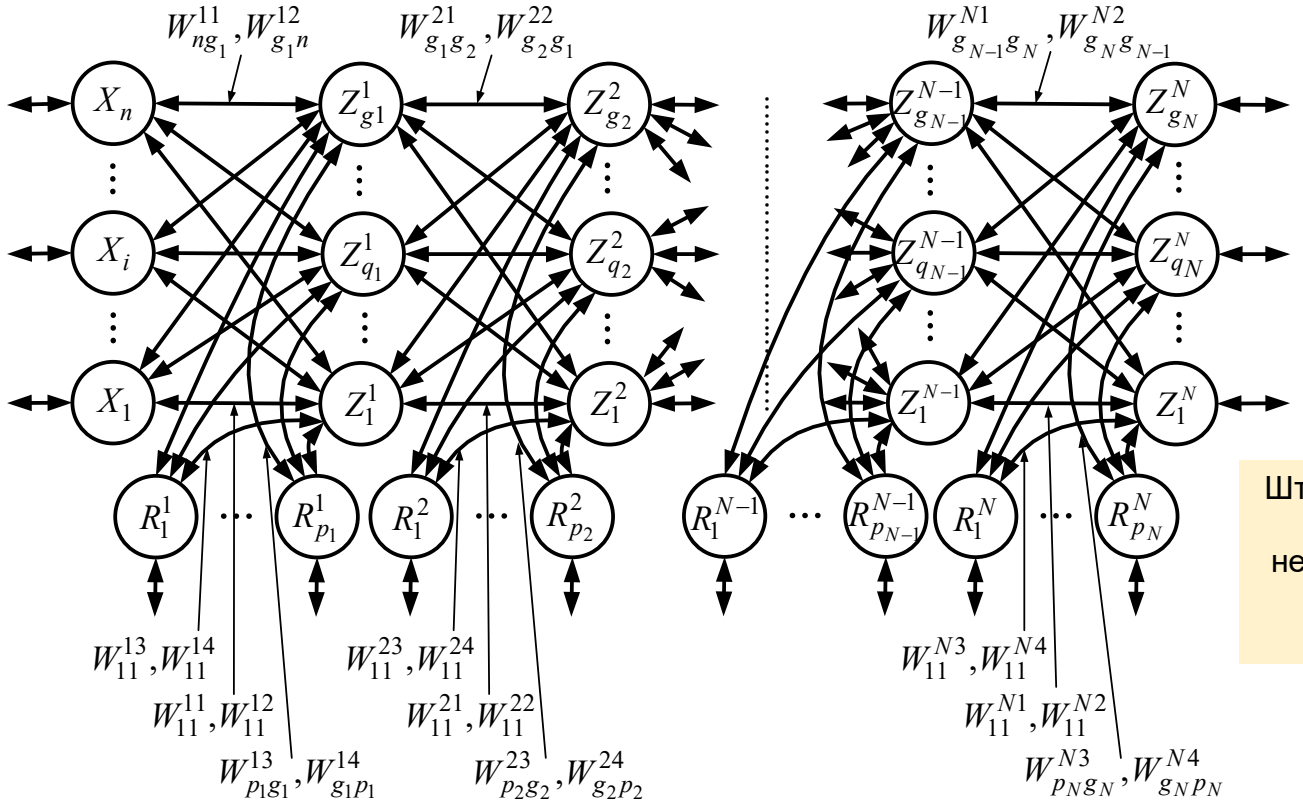


Архітектура тришарового перцептрону, який може довчатися *N* разів

Розроблені нові стабільно-пластичні нейронні мережі Хеммінга, Хебба і мережі на основі перцептрона, котрі, на відміну від їх класичних аналогів, здатні розпізнавати нову інформацію та донавчатися, що дозволяє суттєво розширити область застосування цих нейронних мереж в інтелектуальних системах управління та безпеки об’єктів критичної інфраструктури для автоматизації процесів керування.

НТУ «ХПІ»

ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ БАГАТОКОНТУРНИХ СИСТЕМ БЕЗПЕКИ



Штучна нейромережева багатошарова асоціативна пам'ять з керуючими нейронами, для систем управління та безпеки об’єктів критичної інфраструктури

Розроблено та **запатентовано**: нову базу даних на основі N-направленої та багатошарової асоціативної пам’яті з керуючими нейронами; нову базу знань, котра здатна вхідним векторам ставити у відповідність одну або більшу кількість асоціацій, вирішувати завдання з декількома рішеннями, розпізнавати нову інформацію та донавчатися в процесі функціонування системи. Створено програмне забезпечення, що реалізує розроблені нейронні мережі та дає змогу впровадити отримані теоретичних результатів в системах управління та безпеки об’єктів критичної інфраструктури

НТУ «ХПІ»

МОДЕЛІ УПРАВЛІННЯ ТРАФІКОМ ІНТЕГРАЛЬНИХ ПОТОКІВ ДАНИХ В ІНФО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

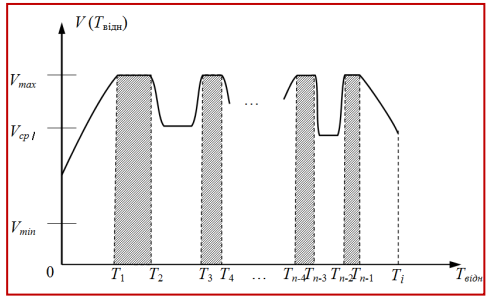
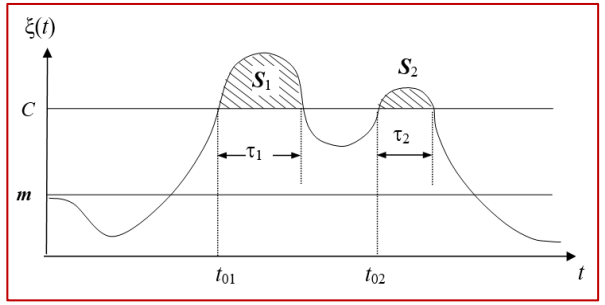


Схема розбиття інтервалу



Викиди трафіку

$$\tilde{W}^{(k,\ell_k)}\left(V_0^{(k,\ell_k)},t\right)=\sum_{(\xi=\overline{0,R-1})}^{(\zeta=\overline{0,N-1})}\alpha_{\zeta,\xi}^{(k,\ell_k)}\cdot L_{\zeta,\Xi}^{(k,\ell_k)}\left(V_0^{(k,\ell_k)}\right)\cdot L_{\xi,Z}^{(k,\ell_k)}(t)=$$

$$=\sum_{(r=\overline{0,R-1})}^{(n=\overline{0,N-1})}m_{n,r}^{(k,\ell_k)}\cdot\sum_{\zeta=0}^{Z}\frac{\Im_\zeta\left(V_0^{(k,\ell_k)}\right)}{\Im_\zeta\left(V_{0,\zeta}^{(k,\ell_k)}\right)}\cdot\sum_{\xi=0}^{\Xi}\frac{\aleph_\xi(t)}{\aleph_\xi\left(t_{n,\xi}\right)},$$

$$\Im_\zeta\left(V_0^{(k,\ell_k)}\right)=\prod_{i=0,\,i\neq\zeta}^{Z}\left(V_0^{(k,\ell_k)}-V_{0,i}^{(k,\ell_k)}\right);\quad\aleph_\xi(t)=\prod_{j=0,\,j\neq\xi}^{\Xi}\left(t-t_{n,j}\right).$$

$$\sum_{(\xi=\overline{0,R-1})}^{(\zeta=\overline{0,N-1})}\alpha_{\zeta,\xi}^{(k,\ell_k)}\times f_{\zeta,\Xi}^{(k,\ell_k)}\left(V_{0,n}^{(k,\ell_k)}\right)\phi_{\xi,Z}^{(k,\ell_k)}(t_r)=m_{mr}$$

$$\rho\left(W^{(k,\ell_k)}\left(V_0^{(k,\ell_k)},t\right),\ \tilde{W}^{(k,\ell_k)}\left(V_0^{(k,\ell_k)},t\right)\right)\le\varepsilon^{(k,\ell_k)};$$

$$\Im^{(k,\ell_k)}=\left[V_{\min}^{(k,\ell_k)},V_{\max}^{(k,\ell_k)}\right]\times\left[0;T^{(k,\ell_k)}\right]\subset\Re^2,\left(V_0^{(k,\ell_k)},t\right)\in\Im^{(k,\ell_k)},$$

$$V^{(k,\ell_k)}(t_0)=\left.\frac{dW^{(k,\ell_k)}(t)}{dt}\right|_{t=t_0}=V_0^{(k,\ell_k)};\quad t\in\left[t_0^{(k,\ell_k)},t_0^{(k,\ell_k)}+T^{(k,\ell_k)}\right],$$

Двовимірна динамічна модель трафіку

$$S_i^{(k,\ell_k)}(t,\beta)=Q_{2\beta+1}^{(k,\ell_k)}(t,j),$$

$$\left.\frac{d^m}{dt^m}Q_{2\beta+1}^{(k,\ell_k)}(t,j)\right|_{t=t_{j,i}^{(k,\ell_k)}}=\left.\frac{d^m}{dt^m}P_\beta\left(t,W_{j,i}^{(k,\ell_k)}\right)\right|_{t=t_{j,i}^{(k,\ell_k)}};$$

$$\left.\frac{d^m}{dt^m}Q_{2\beta+1}^{(k,\ell_k)}(t,j)\right|_{t=t_{j+1,i}^{(k,\ell_k)}}=\left.\frac{d^m}{dt^m}P_\beta\left(t,W_{j,i}^{(k,\ell_k)}\right)\right|_{t=t_{j+1,i}^{(k,\ell_k)}};\ m=\overline{1,\beta}.$$

$$Q_{2\beta+1}^{(k,\ell_k)}(t,j)=P_\beta\left(t,W_{j,i}^{(k,\ell_k)}\right)+R_{2\beta+1}^{(k,\ell_k)}(t,j),$$

$$R_{2\beta+1}^{(k,\ell_k)}(t,j)=(t_{j+1}-t_j)^{\beta+1}\cdot W_{2\beta+1}^{(k,\ell_k)}(t_{j-\gamma},t_{j-\gamma+1},\ldots,t_{j-\gamma+\beta+1})\cdot q_{2\beta+1}(\tilde{t},j),$$

$$q_{2\beta+1}(\tilde{t},j)=\frac{t_{j+\beta-\gamma+1}-t_{j-\gamma}}{t_{j+1}-t_j}\cdot\sum_{r=0}^{\beta}\left(\left.\frac{d^2}{d\tilde{t}^2}\prod_{\xi=0}^{\beta}\left(\tilde{t}-\frac{t_{j-\gamma+\xi}}{t_{j+1}-t_i}\right)\right|_{\tilde{t}=1}\right)\cdot\theta_r(\tilde{t});$$

$$\theta_r(\tilde{t})=\frac{\tilde{t}^{\,j+1}\cdot(\tilde{t}-1)^r}{r!\,j!}\cdot\sum_{m=0}^{\beta-r}(-1)^m\frac{(\beta+m)!}{m!}(\tilde{t}-1)^m.$$

$$P_\beta\left(t,W_{t_{j,i}}^{(k,\ell_k)}\right)=\frac{\sum_{m=0}^{\beta}W^{(k,\ell_k)}\left(t_{m,i}^{(k,\ell_k)}\right)\cdot\prod_{m_1=0}^{\beta}\left(t-t_{m_1,i}^{(k,\ell_k)}\right)}{\prod_{m_2=0}^{m-1}\left(t_{m,i}^{(k,\ell_k)}-t_{m_2,i}^{(k,\ell_k)}\right)\cdot\prod_{m_3=m+1}^{\beta}\left(t_{m,i}^{(k,\ell_k)}-t_{m_3,i}^{(k,\ell_k)}\right)}.$$

Двовимірна сплайн-інтерполяція

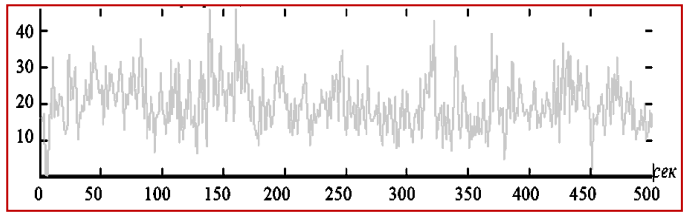
№	Коефіцієнт кореляції $\rho(t)=$	$-\rho_0''$	Частотний спектр коефіцієнта кореляції $S(f)=$
1	$(1+\alpha\lvert\tau\rvert)\times\exp(-\alpha\lvert\tau\rvert)$	α^2	$\frac{4\alpha^3}{\left(\alpha^2+(2\pi f)^2\right)^2}$
2	$\exp(-\alpha\tau^2)$	2α	$\sqrt{\pi/\alpha}\exp\left(-\frac{\pi^2 f^2}{\alpha}\right)$
3	$\left[1+\alpha\lvert\tau\rvert+\frac{1}{3}\times\right.$ $\left.\times(\alpha\tau)^2\exp(-\alpha\lvert\tau\rvert)\right]$	$\frac{\alpha^2}{3}$	$\frac{16\alpha^5}{3}\Big/\left(\alpha^2+(2\pi f)^2\right)^3$
4	$\left(1+(\alpha\tau)^2\right)^{-1}$	$2\alpha^2$	$\frac{\pi}{\alpha}\cdot\exp\left(-\frac{2\pi f}{\alpha}\right)$

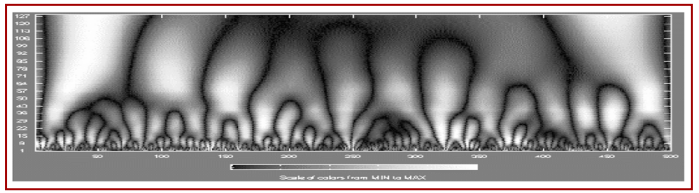
Спектри викидів

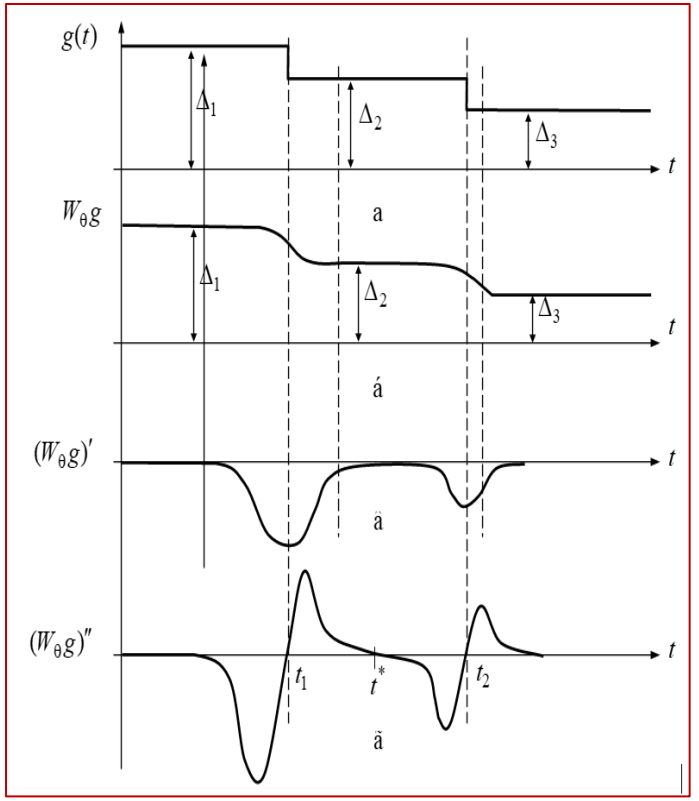
Синтезована двовимірна динамічна модель трафіку інтегрального потоку даних інтелектуальної системи управління об'єктом критичної інфраструктури, котра базується на оперативній статистичній інформації про проходження потоку та припускає наявність даних вимірювань по декількох сесіях. Сумарне відхилення від реального трафіку зменшилося на 15%.

НТУ «ХПІ»

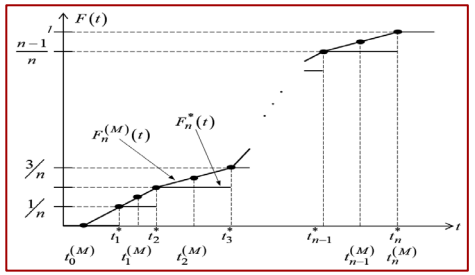
МОДЕЛІ УПРАВЛІННЯ ТРАФІКОМ ІНТЕГРАЛЬНИХ ПОТОКІВ ДАНИХ В ІНФО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ



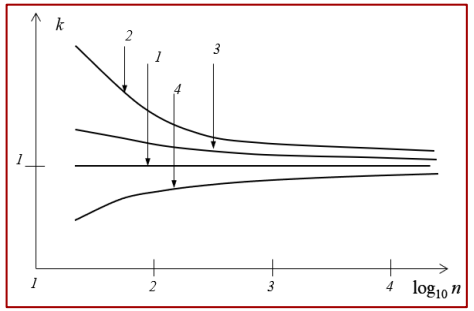




Вейвлет-перетворення та його похідні



Побудова мажоранти



Аналіз результатів

$$F_n^{(M)}(t)=\frac{1}{n}\sum_{l=0}^{n-1}\left(l+\frac{t-t_l^{(M)}}{t_{l+1}^{(M)}-t_l^{(M)}}\right)\left(\Theta\left(t-t_l^{(M)}\right)-\Theta\left(t-t_{l+1}^{(M)}\right)\right)+\Theta\left(t-t_n^{(M)}\right),$$

$$P\left(\sup_t\left(F_n^{(M)}(t)-F(t)\right)\xrightarrow{n\to\infty}\right)=1,$$

$$\Phi\left(f,F_n^{(M)}\right)=\left\|\aleph f-F_n^{(M)}\right\|_{L_2}^2+\alpha_n\Omega(f),\ \aleph^*\left(\aleph f(t)-F_n^{(M)}(t)\right)+\alpha_n f(t)\equiv 0$$

$$\int_{-\infty}^{+\infty}\Theta(x-t)\left(\int_{-\infty}^{+\infty}\Theta(x-\chi)f(\chi)\,d\chi-F_n^{(M)}(t)\right)dx+\alpha_n f(t)\equiv 0.\ (3.41)$$

$$\left(-\frac{1}{ix}+\pi\delta(x)\right)\cdot\left(-\frac{1}{ix}+\pi\delta(x)\right)\widehat{f}(x)-\widehat{F}_n^{(M)}(t)+\alpha_n\widehat{f}(x)=0,$$

$$\widehat{F}_n^{(M)}(x)=\int_{-\infty}^{+\infty}F_n^{(M)}(t)e^{-itx}dt;\ \widehat{f}(x)=\int_{-\infty}^{+\infty}f(x)e^{-ix\chi}d\chi;$$

$$\hat{\Theta}(t-\beta)=\pi\delta(t)-\frac{ie^{-it\beta}}{t};\quad \hat{t\Theta}(t-\beta)=i\left(\pi\delta(1-t)+\frac{ie^{-it\beta}}{t^2}-\frac{\beta e^{-it\beta}}{t}\right),$$

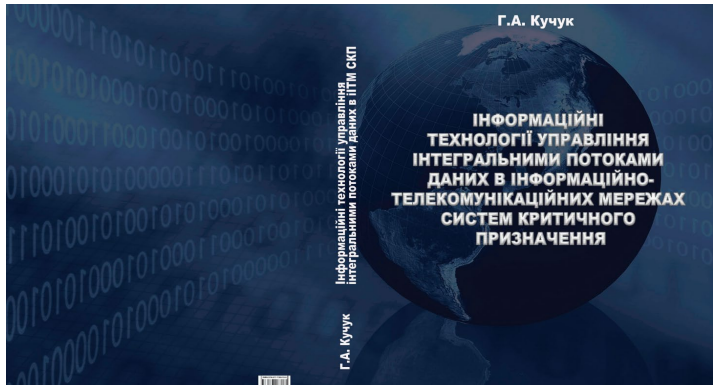
$$\widehat{f}(x)=-\frac{1}{inx\left(1+\alpha_n x^2\right)}\cdot\left(\sum_{l=1}^{n-1}\xi_l\cdot e^{-ixt_l^{(M)}}+\frac{e^{-ixt_n^{(M)}}}{t_n^{(M)}-t_{n-1}^{(M)}}-\frac{e^{-ixt_0^{(M)}}}{t_1^{(M)}-t_0^{(M)}}\right).$$

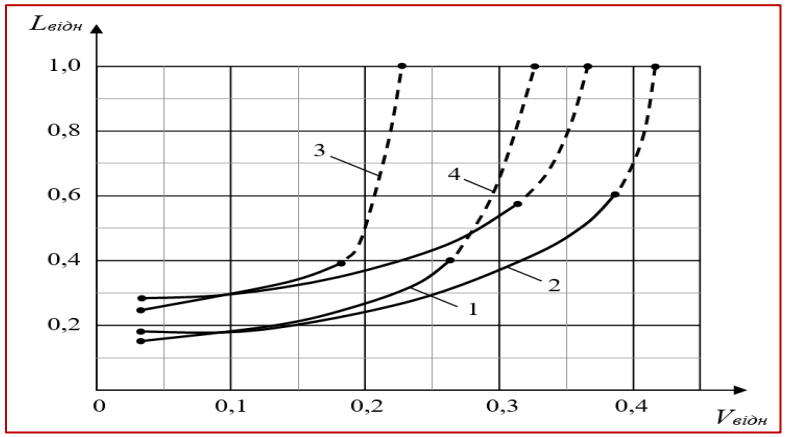
Перетворення трафіку інтегрального потоку даних

Запропонований підхід до оцінки розмірів буферів фільтрації комунікаційного обладнання інфокомунікаційної мережі інтелектуальної системи управління об'єктом критичної інфраструктури, що дозволяє підвищити пропускну здатність віртуальних каналів за рахунок зменшення затримки, яка спричинена підтвердженнями про передачу пакетів, що очікують у чергах комунікаційного обладнання шляхом вибору оптимального розміру буферів фільтрації для інтегральних потоків даних, що обслуговуються.

НТУ «ХПІ»

МОДЕЛІ УПРАВЛІННЯ ТРАФІКОМ ІНТЕГРАЛЬНИХ ПОТОКІВ ДАНИХ В ІНФО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ





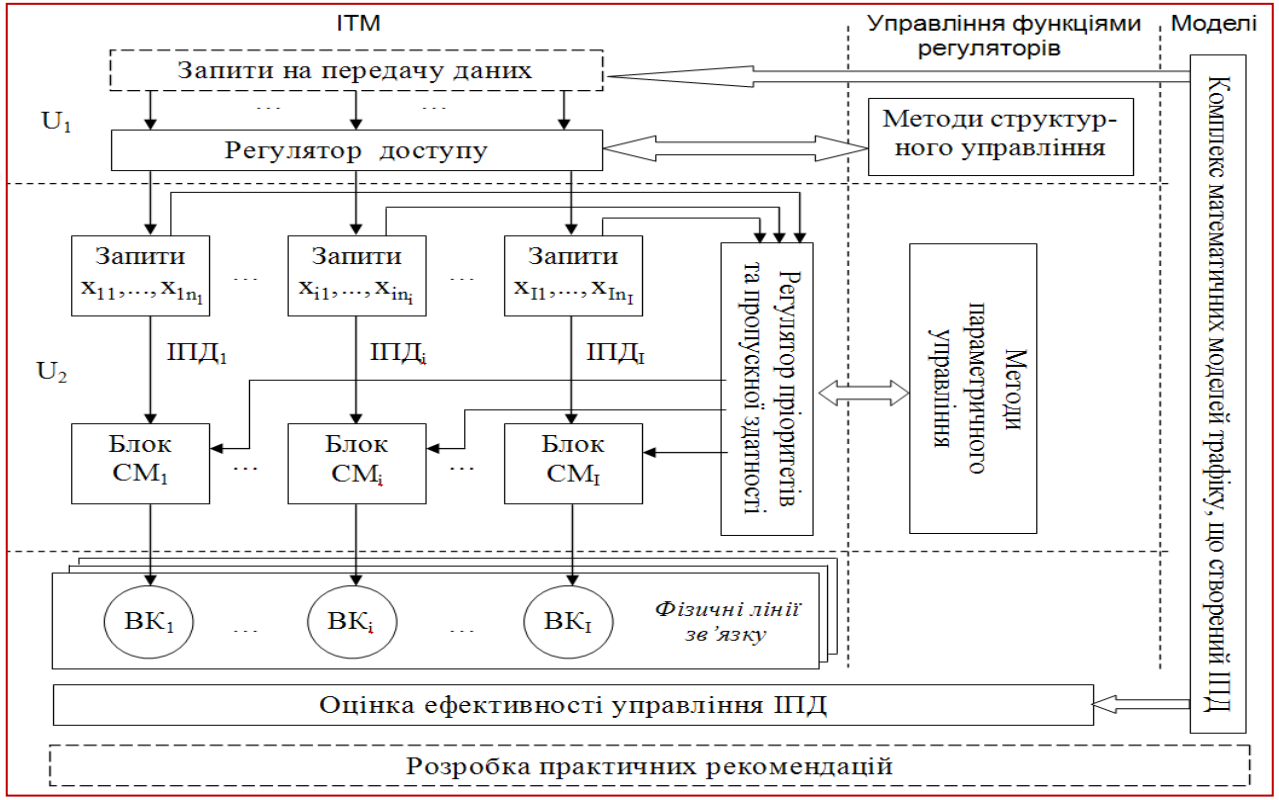
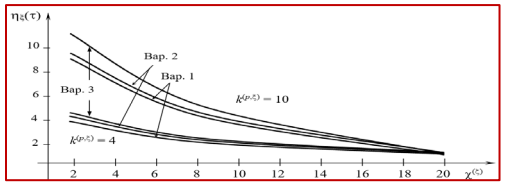


Схема взаємодії технічних і програмних засобів в інфокомунікаційних мережах об'єктів критичної інфраструктури

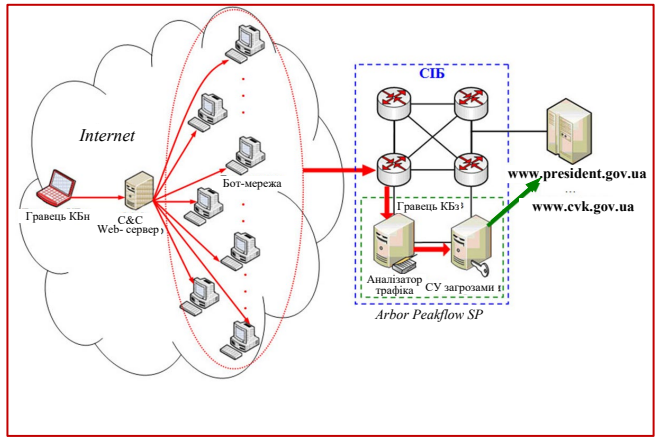
Збільшення потенційних можливостей мережі системи критичного застосування



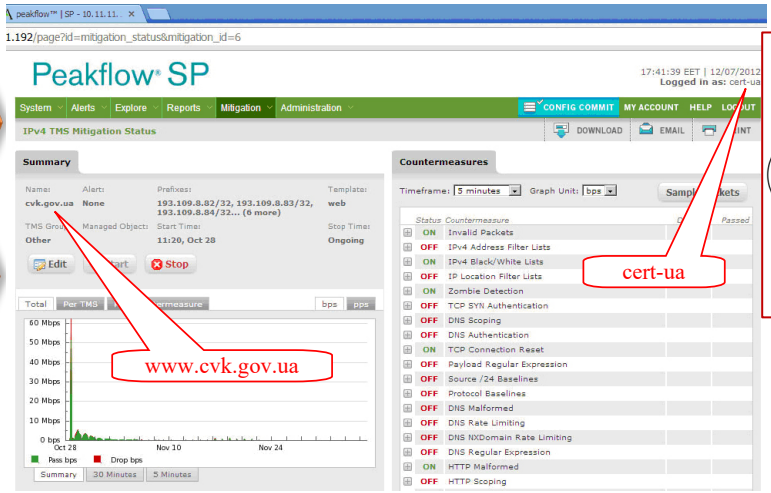
Синтезована математична модель інтелектуального управління трафіком інфокомунікаційних мереж об'єктів критичної інфраструктури на комутаційних вузлах інфокомунікаційної мережі. Використанням оцінки профілю навантаження віртуальних з'єднань з урахуванням фрактального характеру трафіку дозволяє скоротити час обслуговування мережних транзакцій за рахунок вирівнювання рівнів профілю навантаження.

НТУ «ХПІ»

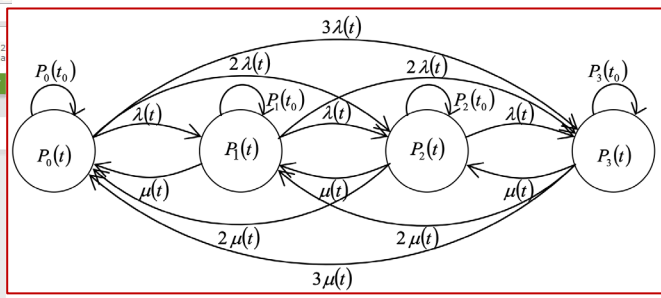
ПРИКЛАДНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНОЇ МЕТОДОЛОГІЇ



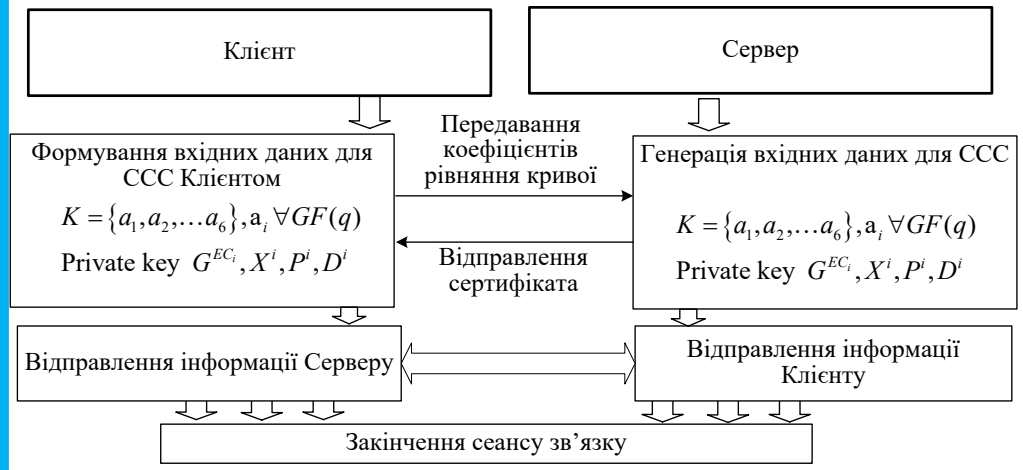
Технологія реалізації процесу кібернападу на державні інформаційні ресурси 28 жовтня 2012 року



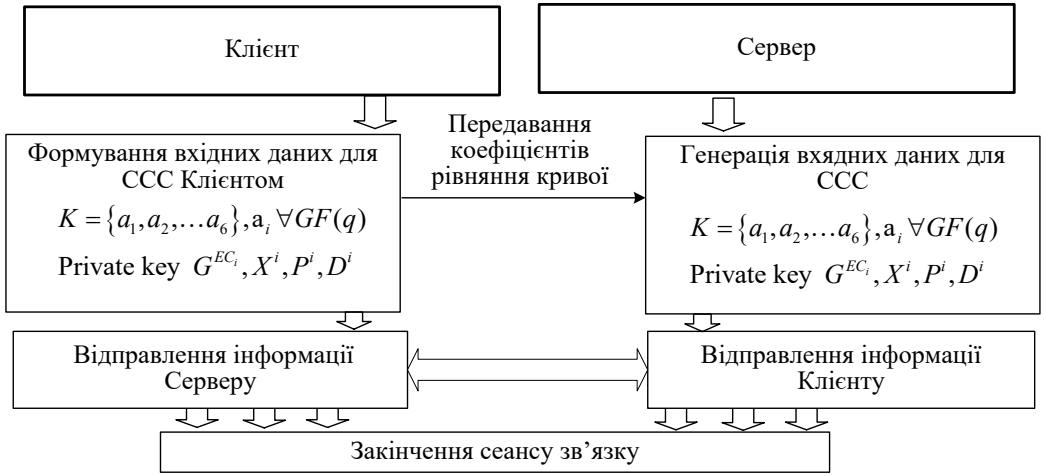
Інтерфейс адміністратора Arbor Peakflow SP



Графова модель шаблону нормальної поведінки Web-сервера Apache 2.2.10 (Linux|SUSE)



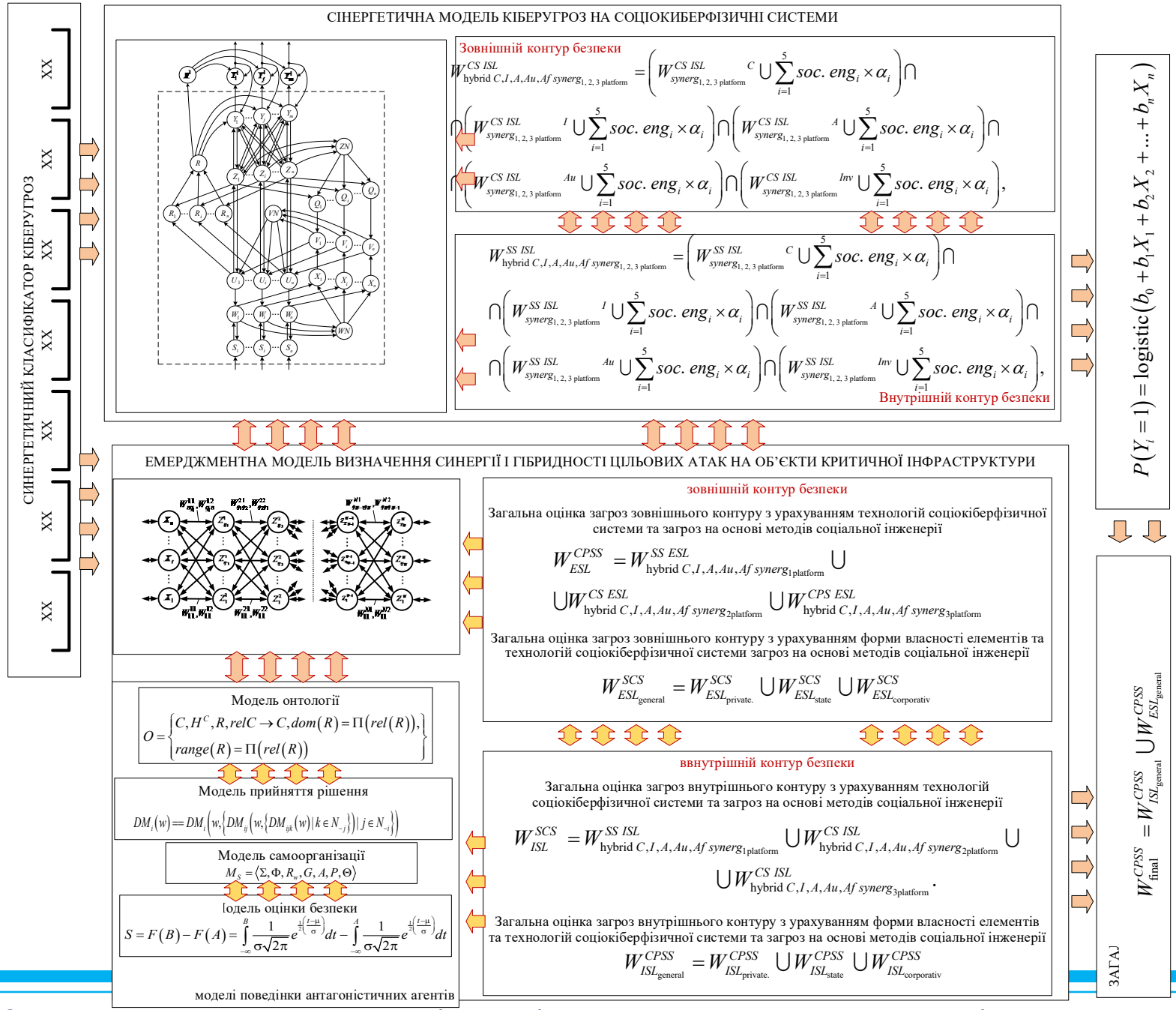
Вдосконалена схема протоколу SSL/TLS



Структурна схема вдосконаленого протоколу SSL/TLS у режимі 0-RTT

НТУ «ХПІ»

ПРИКЛАДНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНОЇ МЕТОДОЛОГІЇ



Запропонована методологія побудови багатоконтурних систем захисту об'єктів критичної інфраструктури забезпечує можливість отримання об'єктивної оцінки поточного стану захищеності об'єктів критичної інфраструктури. Запропонований програмний комплекс оцінки дозволяє отримати інтегрований показник безпеки, виявити критичні точки вразливості та «можливість» зловмисника отримати доступ до конфіденційної інформації.

Структурна схема методології побудови багатоконтурних систем захисту об'єктів критичної інфраструктури

ВИСНОВКИ

У роботі вирішена актуальна науково-прикладна проблема створення принципово нової методології синтезу моделей інтелектуальних систем управління та безпеки об’єктів критичної інфраструктури, що дозволяє підвищити рівень захищеності інформаційних ресурсів цих об’єктів, будувати та /або модернізувати існуючі системи захисту інформації на основі постквантових криптоалгоритмів в умовах комплексування цільових (змішаних) атак з ознаками гібридності та синергізму з методами соціальної інженерії

Вперше розроблено методологію синтезу моделей інтелектуальних систем управління та безпеки об’єктів критичної інфраструктури в основі якої лежить концепція побудови синергетичної моделі загроз та удосконалений класифікатор загроз, методи забезпечення конфіденційності, цілісності та автентичності державних інформаційних ресурсів на гібридних крипто-кодових конструкціях зі збитковими кодами та удосконалений метод оцінювання рівня безпеки інформаційних ресурсів на основі комплексного показника ефективності інвестицій, що дозволило відкрити новий з позицій управління та безпеки, ефективний з позицій витрачених коштів на управління та безпеку підхід до модернізації чинний та створення перспективних інтелектуальних систем управління та безпеки об’єктів критичної інфраструктури держави

Запропонована методологія синтезу моделей інтелектуальних систем управління та безпеки об’єктів критичної інфраструктури надає об’єктивну оцінку будь-якої інфраструктури об’єктів критичної інфраструктури (будь-якої галузі), що забезпечує її універсальність. Виявлена залежність рівня захищеності контуру бізнес-процесів системи безпеки, яка визначається часткою успішно проведених атак по відношенню до їх загальної кількості, від часу перемикання з захисту одного вектору безпеки до іншого, що забезпечує при збільшенні інтервалу на перемикання з одного вектору загроз на інший в 2 рази, кількість успішних атак зменшення в 1,76 рази. При побудові багатоконтурних систем захисту враховують фізичні складові інфраструктури та формують зовнішній та внутрішній контури безпеки.

ВИСНОВКИ

Робота «Методологія синтезу моделей інтелектуальних систем управління та безпеки об’єктів критичної інфраструктури» внесла значний внесок у розробку та впровадження в складові систем управління та безпеки об’єктів критичної інфраструктури, **які є важливими для: національної безпеки та оборони** (складові комплексної системи захисту інформації ЄАСУ ЗС України – для побудови підсистеми захисту інформації в телекомунікаційній системі комплексу засобів автоматизації АСУ бойового управління силами та засобами авіації, протиповітряної оборони всіх видів ЗС України “Ореанда” /замовник – командувач Повітряних Сил ЗС України/, системи і засоби управління військами та зброєю РЕБ /замовник – Командувач Сухопутних військ ЗС України/, системи військового зв’язку АСУ ракетних військ і артилерії /замовник – Командувач Сухопутних військ ЗС України, система забезпечення інформаційної безпеки оперативно-тактичного ракетного комплексу “Гром-2” (ОТРК “Сапсан”) /замовник ДП “КБ “Південне” ім. М. К. Янгеля/); **економіки України** (комплекс засобів захисту інформації телекомунікаційних каналів зв’язку “LDPC-CryptoSuite” /замовник – ТОВ “Мікрокріпт Текнолоджис”/, система Інтернет-банкінгу “ELPay” – для управління та безпечного дистанційного обслуговування клієнтів банків з будь-якої точки світу /замовник – ТОВ “Сайфер”/, системи управління розвитком великих енергохімічних комплексів /замовник – ПАТ “Сумихімпром”/, системи навігації та управління рухом мобільних об’єктів – для оцінювання варіантів побудови перспективних компонент згаданих комплексів /ДП “ЦНДІ навігації і управління” Мінпромполітики України/.