[11]. Khemapech I., Miller A., Duncan I. A survey of transmission power control in wireless sensor networks.
Proceedings of PGNet, 2007. P. 15-20.
[12]. Hung C. W. et al. Transmission power control in wireless sensor networks using fuzzy adaptive data rate.
Sensors. 2022. Vol. 22, no. 24. [Online]. Available: https://www.mdpi.com/1424-8220/22/24/9963.

ADAPTIVE INTERFERENCE SUPPRESSION IN WIRELESS NETWORKS BASED ON ARTIFICIAL NOISE

Adaptive interference suppression based on artificial noise is a promising approach to enhancing the security of wireless networks. In traditional cryptographic protection systems, attackers can exploit physical-layer attacks to intercept signals. One of the effective protection methods is the use of artificial noise (AN), which generates specially designed interference to complicate unauthorized access. This paper investigates the principles of adaptive artificial noise power control using the gradient descent method. The proposed approach enables dynamic noise level regulation based on communication channel parameters such as attacker distance, signal strength, and environmental interference. The modeling was conducted using an open-source wireless sensor network (WSN) dataset, allowing us to evaluate the impact of adaptive noise on packet loss and signal strength. The results demonstrate that the optimized method effectively reduces the probability of interception without significantly degrading the communication quality for legitimate users. The proposed model can be applied in modern mobile communication systems, IoT networks, and critical infrastructures requiring an increased level of data protection.

Keywords: interference suppression, artificial noise, wireless sensor networks.

Кудренко Станіслава Олексіївна, к.т.н., доцент, доцент кафедри комп'ютерних систем та мереж, Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», м.Київ, Україна.

Stanislava Kudrenko, Candidate of Technical Sciences, associate professor of the Department of Computer Systems and Networks of the State non-commercial company state university «Kyiv aviation institute», Kyiv, Ukraine.

E-mail:stanislava.kudrenko@npp.nau.edu.ua.
ORCID ID: 0000-0002-0759-3908.

Козловський Валерій Валерійович, д.т.н., професор, завідувач кафедри технічного захисту інформації, Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», м. Київ, Україна.

Valeriy Kozlovsky, head of the Department of Technical Information Protection of the State non-commercial company state university «Kyiv aviation institute», Kyiv, Ukraine.

E-mail:valerii.kozlovskyi@npp.kai.edu.ua.
ORCID ID: 0000-0002-8301-5501.

Столяр Анна Леонідівна, аспірантка кафедри комп'ютерних систем та мереж, Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», м.Київ, Україна.

Anna Stoliar, PhD student of the Department of Computer Systems and Networks of the State non-commercial company state university «Kyiv aviation institute», Kyiv, Ukraine.

E-mail: stoliarannanau@gmail.com.
ORCID ID: 0000-0002-7669-1202.

УДК 004.621.3

КЕРУВАННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ У СИСТЕМІ КІБЕРЗАХИСТУ

Андрій Фесенко, Наталія Вишневська, Діана Козловська

Досліджено методи керування інформаційними потоками в системах кіберзахисту з використанням ймовірнісних моделей та алгоритмів оптимізації. Розроблено математичний апарат для аналізу та стабілізації потоків даних у багатоканальних системах. Використано марківські ланцюги для моделювання фазових станів потоків, математично оцінили інформаційні характеристики системи, коефіцієнти стискання та інтервали квазістаціонарності. Розглянуто вплив параметрів допуску, ймовірностей фазових станів і рівнів дискретизації на передачу інформації. Введено механізми регулярізації для уникнення сингулярностей та забезпечення стабільності роботи системи. Запропоновано

адаптивний підхід до управління потоками, що дозволяє динамічно коригувати параметри системи в умовах зміни загроз і збереження точності передачі даних.

***Ключові слова**: кіберзахист, інформаційні потоки, марківські ланцюги, інформаційна характеристика, коефіцієнт стискання, регуляризація, адаптивне управління, квазістаціонарність, прогнозування ,оптимізація, системи передачі даних.*

Вступ.

Сучасний світ переживає період стрімкої цифровізації. Новітні технології проникли в усі сфери життя, створюючи як нові можливості, так і виклики. Кібернетичний і інформаційний простір стали невід'ємною частиною економічного та соціального розвитку країни. Проте разом із перевагами цифровізації виникли й серйозні загрози, зокрема кібератаки та порушення інформаційної безпеки. Для України ця проблема є особливо актуальною. Сучасний стан держави та підвищений ризик кібератак вимагають оперативних та ефективних рішень у сфері кіберзахисту. Нові технологічні виклики змушують адаптуватися та впроваджувати інноваційні підходи до управління інформаційними потоками в системах кіберзахисту. Це питання стає актуальним у забезпеченні безпеки як державних, так і приватних структур.

Мета даної роботи є розробка методів управління інформаційними потоками в системах кіберзахисту задля підвищення їх ефективності в умовах динамічних загроз.

У умовах стрімкого розвитку інформаційних технологій та цифрових комунікацій актуальність проблеми кіберзахисту зростає з кожним роком. Складність і динамічність також вимагають впровадження нових підходів до управління інформаційними потоками. Аналіз методів управління інформаційними потоками вказує на актуальність трьох основних підходів: детермінованих, ймовірнісних та методів на основі машинного навчання. Детерміновані методи характеризуються високою точністю та стабільністю роботи в умовах системи фіксованих параметрів. Вони застосовуються для захисту стабільних мереж із передбачуваними навантаженнями, проте демонструють обмежену ефективність у разі динамічних змін. Ймовірнісні методи базуються на аналізі статистичних характеристик трафіку і здатні виявляти відхилення від нормальної системи поведінки. Вони є більш адаптивними до змін середовища, проте потребують значних обчислювальних ресурсів. Методи на основі машинного навчання і штучного інтелекту демонструють здатність до автоматичного виявлення аномалій, аналізу поведінки користувачів і прогнозування наведених загроз. Їх переваги можуть у здатності вчитися на нових зразках даних, що забезпечують ефективність протидії новим типам атак. Однак ці методи вимагають постійного оновлення моделей і можуть бути чутливими до якості навчальних даних. [8]

Для дослідження вибрано ймовірнісні методи управління інформаційними потоками через їх здатність адаптуватися до умов динамічних загроз та опрацьовувати невизначеності, які можна оцінити ймовірностями. Ці методи дозволяють оцінювати ймовірність виникнення аномалій, прогнозувати їх розвиток і своєчасно реагувати на них у реальному часі, що є критичним місцем для забезпечення безпеки інформаційних систем. Завдяки цьому вони забезпечують не лише фіксацію порушень, але й запобігання їхньому впливу, сприяючи підвищенню стійкості мережевої інфраструктури. Ймовірні підходи демонструють високу ефективність навіть за умови значної варіативності параметрів трафіку, що робить їх ефективними для сучасної мережі, де прогнозування та виявлення аномалій є ключовими для збереження стабільності системи. [8]

Сучасні підходи до управління кібербезпекою що ґрунтуються на ймовірнісних моделях, та описують процеси й захист об’єктів такі як фазові координати. Завдяки технічному прогресу досягається висока точність моніторингу й управління системами кіберзахисту. Це дає змогу вчасно оцінити стан елементів системи та прийняти відповідні рішення. Однак мінливість умов роботи вимагає впровадження багаторівневих і багатоканальних технологій для обробки інформаційних потоків. Вони дозволяють системам зберегти ефективність навіть за умов постійних змін характеристик каналів зв'язку. Урахування конкретних прикладів загроз, таких як DDoS-атаки на критичну інфраструктуру, витік конфіденційної інформації через

фішингові атаки, а також використання шкідливого програмного забезпечення, забезпечує прикладне значення дослідження та демонструє його практичну значущість. [1,2,8]

Основна частина.

У сучасних інформаційних системах обсяг даних, що передається через мережу, постійно зростає. Разом з цим зростає й ризик кіберзагроз, таких як DDoS-атаки, аномальний трафік, витоки інформації та інші. Ефективне управління інформаційними потоками відіграє важливу роль для підтримки стабільності та безпеки мережі. Основним завданням є оптимізація потоків з одночасним збереженням точності передачі даних та мінімізації витрат.

У практиці багатоканальних систем контролю, використання рівномірного циклічного формування повідомлень дозволило забезпечити гнучко управління трафіком навіть за умов значної варіативності параметрів каналів зв'язку. Це необхідність обумовлена зростанням вимог до мінімізації обсягу інформаційного потоку, збереження вихідної інформації або зменшення її витрат. Інтеграція багаторівневих технологій із ймовірними методами дає можливість ефективно аналізувати динаміку потоків, виявляти аномалії та застосовувати коригувальні рішення. Визначимо інформаційність циклічного потока повторним виразом [3]:

$$\theta = \sum_{i=1}^{k_1} \omega_{oi} \sum_{j=1}^{k_2} m_{ij}\theta_j$$

де θ – адекватність інформації на один вимір при j- м значенні дозволяючої спроможності та частоти опитування; k_1 – число частот опитування, k_2 – число дозволяючих здатність каналів; ω_{oi}=$\omega_{oi}[f(t), \varepsilon(t)]$ – частота опитування каналу, що визначає найбільшу ширину спектра функції $f(t)$ та максимальної доступної помилки $\varepsilon(t)$, m_{ij},- ваговий коефіцієнт, що враховує взаємодію i частоти опитування j-го каналу. θ_j - адекватність інформації для j -го каналу.

Добре відомі надлишки циклічного потоку, примушуючого здійснювати стискання переказуємого та оброблюємого повідомлення. Зниження інтенсивності потоку інформації за рахунок стиснення робить останній не тільки випадковим, але й нестаціонарним. Теоретичні та експеременталні дослідження багатоканальних систем зі списком даних дозволяє, зокрема рахувати результуючі потоки нестаціонарним пуасоновським. [4] Ця обставина ускладнює їх раціональне обслуговування (переказ та обробка) без введення керуючих впливів, розрахованих на компенсацію відмінності від нормального навантаження системи обслуговування. У випадках що мають практичний інтерес, нестаціонарність стислого потоку носить повільний характер та при високій швидкості обслуговуючих пристроїв з квазістаціонарними властивостями. Керування таким потоком не потребує безперервного вимірювання його інтенсивності усереднені інтервала квазістаціонарності

$$\alpha(\tau) = const, \forall\tau \in \left[-\frac{\mathrm{T}}{2}, \frac{\mathrm{T}}{2}\right] \quad (2)$$

де α(τ) - характеристика, наприклад, інтенсивність потоку, що залишається сталою; Т – інтервал квазістаціонарності, та заснований на контролі інтенсивності тільки на межах цих інтервалів. Якщо Т занадто малий, система буде надто чутливою до короткочасних змін, що може викликати слабку реакцію і навпаки якщо Т занадто великі, можуть виникати затримки в адаптації до змін, що знижує ефективність керування.

$$\mathrm{T} = \frac{\text{середня частота зміни інтенсивності}}{\text{середня тривалість сталого стану}} \quad (3)$$

де середня тривалість сталого стану — це час, протягом якого система залишається стабільною (без значних змін параметрів), а середня тривалість сталого стану - це частота, з якою інтенсивність потоку постійно змінюється.

Для оцінки ефективності передачі інформації в багатоканальних системах, дозволяючи встановлювати залежність між параметрами точності передачі даних і всією інформацією, а також оптимізації допусків для досягнення необхідного рівня інформаційної системи, за умов обмежених ресурсів, використовують інформаційну характеристику N - канальної системи, яка є показником загальної ефективності передачі інформації через множину каналів з урахуванням заданих параметрів точності, скористаємось формулою:

$$\Theta_k = \sum_{q=1}^{N} log\,\frac{100}{\varphi_a} \quad (4)$$

де Θ_k - представляє сукупний внесок усіх каналів до загальної інформаційної системи.

$\log\frac{100}{\varphi_a}$ визначає внесок кожного окремого каналу, φ_a - допуск на істотність змін, вираженим у відсотках. Допуск характеризує рівень точності або деталізації, з яким інформація передається через канал. Чим меншим є значення допуску, тим більший рівень точності передачі даних, і, відповідно, тим більший внесок каналу до загальної інформаційної системи." k" - коефіцієнт пропорційності, який визначається експериментальним шляхом. q є змінною, що дозволяє узагальнити розрахунок інформаційної характеристики для всієї багатоканальної системи шляхом завершення внеску кожного окремого каналу. N - загальна кількість каналів.

Щоб уникнути процесу необґрунтованого підбору допусків і забезпечити досягнення номінального значення інтенсивності λ_H– вибір залежності між параметрами $\{\varphi_q\}$ і введеної інформаційною характеристикою Θ_k Дійсно як Θ_k , так і поточне значення інтенсивності $\lambda_T = \sum_{q=1}^{N}\lambda_q$ є функціями $\{\varphi_q\}$, отже, існує залежність $\Theta_k = \Theta_{k(\lambda_T)}$.

Лінеаризуючи цю залежність в оточенні λ_H отримуємо

$$\Theta_{kH} = \Theta_{Tk} + k(\lambda_H - \lambda_T) \quad (5)$$

де Θ_{kH} —значення інформаційної характеристики, необхідне для забезпечення компенсації відхилення поточного значення інтенсивності λ_T від номінального λ_HТобто для досягнення необхідного рівня інформаційності потрібно змінювати допуски φ_q на окремих каналах таким чином, щоб значення Θ_k приймало значення Θ_{kH}.

Переналаштування виконується шляхом додаткової зміни допусків, що дозволяє поступово досягти необхідного значення інформаційної характеристики без прямої інтенсивності коригування. λ_T. Такий підхід має перевагу у швидкості реакції, після уникнення середнього вимірювання λ_T значно скорочує час, необхідний для прийняття керуючих рішень. Це забезпечує меншу інерційність системи та знижує ризики, пов'язані з переповненням буферів або іншими обмеженнями.

Таким чином, визначене у результаті зміни поточної інтенсивності її відхилення від номіналу використовується разом з поточним значенням інформаційної характеристики щодо визначення нового Θ_{kH}, вимагаємого для компенсації відхилення інтенсивності: необхідно так змінити допуски на елементарні потоки, щоб Θ_k у (2) прийняла значення Θ_{kH}. Це можливо досягти, послідовно змінюючи допуск по окремих каналах таким чином, щоб поступово наблизитися не до безпосереднього значення інтенсивності потоку, а до необхідного значення інформаційної характеристики системи. Такий підхід дозволяє уникнути різких змін параметрів передачі даних, забезпечуючи більш плавну адаптацію до змінних умов роботи. При цьому досягається значний виграш у часі реагування, оскільки на кожному кроці керування немає необхідності безпосередньо вимірювати поточне значення λ_T, яке зазвичай змінюється набагато швидше, ніж виконується обчислення інформаційної характеристики засобами ПЕОМ. Це знижує затримки в процесі ухвалення рішень і дозволяє більш ефективно керувати інформаційними потоками без зайвих витрат обчислювальних ресурсів (2).

У результаті інерційність керування зменшується на ті ж порядки, що сприяє зниженню можливості переключення або очищення буфера. Вартість керування при цьому має подвійний характер, допускаючи «обмін» часу реалізації курування на вимагаємую величину для нього, ця величина знаходиться у пам’яті яку попередньо розрахували та розмістили у пам’яті у таблиці $\Theta_k(\overline{\varphi})$. Обсяг такої таблиці буде тим менше, а її використання тим зручніше, чим ширший допусковий інтервал інтенсивності, в межах якого немає потреби здійснювати її регулювання. Це говорить про те, що при достатньо широкому інтервалі допустимих змін інтенсивності можна зменшити кількість необхідних налаштувань і спростити процес адаптації системи. Відповідно, знижується обсяг обчислювальних ресурсів, необхідних для коригування параметрів, що сприяє підвищенню загальної ефективності роботи системи. Визначемо також, що λ_{noT} та λ_H – скалярні функції векторного аргумента $\overline{\varphi} = (\varphi_1, \varphi_2, \dots, \varphi_N,)$ де φ_q – допуск на існування для q – го каналу. Для чого, крім обмежень на екстремум, завжди повинна виконуватися умова $\varphi_i \le \varphi_j$ при $i < j$, що забезпечує реалізацію правила вибору установок алгоритму формування. Θ_k – регуляна функція $\overline{\varphi}$

інваріантія відносно заміни φ_i на φ_j та φ_j на φ_i в той же час як $\lambda_{пот}(\overline{\varphi})$ випадкова та неінваріантною до такої заміни. Звідки виходить, що зв'язок λ та Θ_k (не функцій $\overline{\varphi}$) носить емпіричний регресивний характер.

Ідея керування при цьому у переналаштуванні цього алгоритму, формування сумарного потоку за рахунок поканального змінення допусків на неістотність змін та проводить до наступної задачі: визначити правило зміни канальних дозволів спроможності, що забезпечує задану величину потоку та максимізуючи при цьому його інформацію.

З урахуванням стиснення інформативність потоку існуючих відрахунків

$$\Theta = \sum_{q=1}^{N} \lambda_q \, log \, \beta_q \approx \frac{\lambda_T}{N} \sum_{a=1}^{a_{max}} N_a \, log \frac{100}{\varphi_a} = \frac{\lambda_T}{T} \Theta_k \qquad (6)$$

$$P_{ij} = \|P_{ij}\|, P_{ij} = \begin{cases} 0 \text{ при } |i-j| \geq 2, \\ 1 - P_q \text{ при } i = j, \\ P_q/_2 \text{ при } |i-j| = 1, (1 < i < m), \\ P_q \text{ при } |i-j| = 1, \ i = 1 \text{ та } i = m, \end{cases} \qquad (7)$$

де $i, j = 1,2,\dots,m$ отримуємо зв'язок між коефіцієнтами стиснення K_q по кожному напряму $q = 1,2,\dots,N$ та допуском на неістотність φ_q

Коефіцієнт стискання потоку описує залежність коефіцієнта стискання від параметрів точності передачі інформації, ймовірності станів та рівня дискретизації даних. Тобто K_q є мірою ефективності зменшення обсягу інформаційного потоку з урахуванням заданих характеристик системи, і розраховується за формулою:

$$K_q = \frac{\varphi_q}{P_q} \cdot \frac{m-1}{1-\varphi_q} \qquad (8)$$

де φ_q – допуск на неістотність змін для q-го каналу і визначає ступінь деталізації переданої інформації. Зменшення допуску збільшує точність передачі, але вимагає більше ресурсів для її обробки. Водночас підвищення допуску призводить до втрати деталізації, що знижує інформаційність потоку, P_q— ймовірність фазового стану, враховує статистичний характер змін в інформаційному потоці, що дозволяє коригувати модель відповідно до реальних умов передачі даних. m— кількість рівнів квантованого сигналу визначає дискретність представлення сигналу і λ_q – інтенсивність потока по q – му каналу; $\beta_q = \frac{100}{\varphi_a}$ – загальне число рівнів квантування істотного вимірювання; φ_a – допуск на істотність (у відсотках від шкали); N_a – число каналів з допуском φ_a; N – загальне число каналів.

Для отримання аналітичної залежності між сукупністю допусків та інтенсивністю потоку даних необхідно зробити припущення щодо характера зміни процесів, тобто побудувати їх математичну модель.

Відомо [5,6,7], що Марківські представлення використовуються при більшості реальних процесів. Приймаємо у якості моделі квантованого по часу та рівно процесу Марківського ланцюга з матрицею, маємо

прямо впливає на точність відтворення інформації.

Для запобігання сингулярності у випадках, коли $\varphi_q \to 1$, що може призвести до ділення на нуль у знаменнику, доцільно використовувати регуляризовану форму:

$$K_q = \frac{\varphi_q}{P_q} \cdot \frac{m-1}{max(1-\varphi_q, \epsilon)}, \qquad (9)$$

де $\epsilon > 0$ – мале додатне число, яке запобігає виникненню некоректних результатів у крайових випадках.

Подальший аналіз дозволяє узагальнити розрахунок для всієї системи, визначаючи загальний коефіцієнт стискання K для N каналів, описаних однаковими частотними характеристиками. Це дає змогу оцінити середньозважений вплив кожного каналу на загальний коефіцієнт стискання, враховуючи ймовірність зайнятості ресурсу φ_q, потужність каналу P_q і співвідношення між числом можливих станів системи m та їх невикористаними станами.

$$K = \frac{1}{N} \sum_{q=1}^{N} \frac{\varphi_q}{P_q} \cdot \frac{m-1}{1-\varphi_q} \qquad (10)$$

Для стабілізації потоку на основі формули (10) необхідно попередньо знати типове співвідношення ймовірностей P_q для всіх

каналів ($q = \overline{1, N}$).

Зміни загального коефіцієнта K обумовлюються змінами P_q у процесі роботи системи. Проте основна мета моделі — стабілізація сумарного потоку, а не окремих потоків для кожного каналу. Це досягається рівномірним зменшенням усіх P_q, при цьому зберігається початковий баланс між каналами.

Для адаптації системи до поточних змін у параметрах сигналів підбирається новий набір допусків P_q. Підбір здійснюється таким чином, щоб компенсувати відхилення коефіцієнта стискання від його номінального значення. При цьому враховуються всі необхідні співвідношення між компонентами вектора $\overline{\varphi}$. Що дозволяє динамічно оптимізувати інформаційні потоки в багатоканальних системах шляхом налаштування параметрів стискання. Вона забезпечує адаптивність системи до змінних умов роботи, зберігаючи необхідний рівень ефективності передачі даних. Для отримання аналітичної залежності між сукупністю допусків та інтенсивністю потоку даних необхідно зробити припущення щодо характера зміни процесів, тобто побудувати їх математичну модель.

Висновки

У статті представлено ймовірнісні методи управління інформаційними потоками, які забезпечують адаптацію системи до змінних умов і можуть виявляти аномалії в реальному часі. Запропоновані підходи базуються на математичних моделях, що враховують динаміку мережевого трафіку, та спрямовані на оптимізацію передачі даних і зменшення втрат інформації. Методи, описані в роботі, дозволяють інтегрувати багаторівневі та багатоканальні технології, які підтримують стабільність роботи системи навіть за умов зміни параметрів трафіку. Отримані результати можуть бути основою для розробки систем кіберзахисту, які адаптуються до поточних умов та реагують на загрози. Подальший розвиток дослідження розробки інтеграції моделей з урахуванням залежностей між попередніми і поточними станами системи для покращення прогнозування та управління потоками даних.

Література:

[1] Козюра В.Д. Захист інформації в комп'ютерних мережах/В.Д. Козюра, В.О. Хорошко, М.Є. Шелест та інші – Ніжин: ТПК «Орхідея», 2020, – 236с.

[2] Козюра В.Д. Процеси та технології в інформаційних системах/ В.Д. Козюра, Л.М. Скачек, Ю.М. Ткач та інші – Ніжин: ТПК «Орхідея», 2020, – 278с.

[3] Юр'єв Ю.М. Концепція мережі авіаційного електрозв'язку /Ю.М. Юр'єв//Проблеми підвищення ефективності інфраструктури. Збірник наукових праць – К:НАУ, Вип.6, 2001 – С:118-125.

[4] Литвинов В.В. Математическое обеспечение проектирования в вычислительных сетей//В.В. Литвинов – К: Техніка ,1982. – 216с.

[5] Згуровський М.З. Основи системного аналізу/М.З. Згуровський, Н.Д. Панкратова – К:Вид. група BHV, 2007. – 544с.

[6] Дибкін Є.Б. Марківські процеси/Є.Б. Дибкін – К:Наукова думка, 1999. – 860с.

[7] Стратонович Р.Л. Умовні марківські процеси та їх застосування/Р.Л. Стратонович – К:КНУ ім. Татарса Шевченка, 2001. – 322с.

[8] Шульга В.П., Іванченко Є.В., Вишневська Н.С., Бербер А.С. Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави/ Сучасний захист інформації., 2024, №3(59), https:// DOI: 10.31673/2409-7292.2024.030001.

MANAGEMENT OF INFORMATION FLOWS IN A CYBERSECURITY SYSTEM

Methods for controlling information flows in cybersecurity systems using probabilistic models and optimization algorithms have been studied. A mathematical framework has been developed for analyzing and stabilizing data flows in multichannel systems. Markov chains have been used to model the phase states of flows, and the information characteristics of the system, compression coefficients, and quasi-stationarity intervals have been mathematically estimated. The influence of tolerance parameters, phase state probabilities, and discretization levels on information transfer has been considered. Regularization mechanisms have been introduced to prevent singularities and ensure system stability. An adaptive approach to flow control has been proposed, allowing for dynamic adjustment of system parameters in the face of changing threats while maintaining the accuracy of data

transmission.

Keywords: cybersecurity, information flows, Markov chains, information characteristics, compression coefficient, regularization, adaptive control, quasi-stationarity, forecasting, optimization, data transfer systems.

Фесенко Андрій Олексійович, кандидат технічних наук, доцент, декан факультету комп'ютерних наук та технологій, Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», м. Київ, Україна.

Andriy Fesenko, PhD in Technical Sciences, Associate Professor, Dean of the Faculty of Computer Science and Technologies of the State non-commercial company state university «Kyiv aviation institute», Kyiv, Ukraine.

E-mail: aafesenko88@gmail.com.

ORCID ID: 0000-0001-5154-5324.

Вишневська Наталія Сергіївна, старший викладач кафедри кібербезпеки, , Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», м. Київ, Україна.

Nataliya Vyshnevska, senior Lecturer at the Department of Cybersecurity of the State non-commercial company state university «Kyiv aviation institute», Kyiv, Ukraine.

E-mail: nataliia.vyshnevska@npp.kai.edu.ua.

ORCID ID: 0000-0002-1358-467X.

Козловська Діана Валеріївна, студентка 3 курсу факультету комп'ютерних наук та технологій, Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», м. Київ, Україна.

Diana Kozlovska, third-year Student of the Faculty of Computer Science and Technologies of the State non-commercial company state university «Kyiv aviation institute», Kyiv, Ukraine.

E-mail: vvkzeos@gmail.com.

ORCID ID: 0009-0004-6223-0319.

УДК 004.056

ПРОВЕДЕННЯ СТУДЕНТСЬКИХ ОЛІМПІАД ТА ІНШИХ ЗМАГАНЬ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВПРОВАДЖЕННЯ ЇХ НАПРАЦЮВАНЬ У НАВЧАЛЬНИЙ ПРОЦЕС

Валентин ПЕТРИК

Описується мета, методика та система оцінювання Міжнародної студентської олімпіади «Шляхи та механізми захисту інформаційного простору України від шкідливих інформаційно-психологічних впливів» і Всеукраїнської студентської олімпіади «Формування критичного мислення шляхом виявлення достовірної, недостовірної, частково достовірної та можливо достовірної інформації» (інша назва «Соціоінженерінг: шляхи та механізми захисту»). Описується VII Міжнародна конференція «Захист демократичних цінностей і дотримання прав людини у діяльності спецслужб» за спеціалізацією «Російська агресія проти України, як фундаментальна загроза свободі, цінностям демократичного суспільства і правам людини: український, європейський та світовий контексти». Показано практичну значимість цих змагань, яка забезпечується завдяки впровадженню в освітній процес ВНЗ результатів їх напрацювань. Розробляються пропозиції щодо проведення нових студентських олімпіад, а саме з не технічних аспектів інформаційної безпеки, а також релігієзнавства.

Ключові слова: *студентські олімпіади, шкідливі інформаційно-психологічні впливи, захист інформаційного простору, інформаційна безпека, інформаційно-психологічне протиборство.*

Вступ

На сьогодні більша частина матеріалів вітчизняних наукових заходів з інформаційної безпеки (наукових, науково-практичних конференцій та семінарів, а особливо студентських олімпіад) не мають практичного використання. Більшість напрацювань цих заходів необхідно проваджувати у виробництво або навчальний процес. Не доцільно друкувати збірки тільки для аспірантів, докторантів та вузького кола фахівців, що використовують для написання дисертацій, монографій, наукових статей або нерідко видають для звітності (потім ці матеріали ні ким і ні коли не використовуються).

У розпорядженні Кабінету Міністрів України