КРИПТОЛОГІЯ / CRYPTOLOGY

DOI: 10.18372/2225-5036.27.16001

МЕТОД СКРЕМБЛЮВАННЯ СИСТЕМИ СЛУЖБОВИХ СКЛАДОВИХ КРИПТОКОМПРЕСІЙНИХ КОДОГРАМ

Володимир Бараннік[1], Сергій Сідченко[2], Валерій Бараннік[3] Андрій Хіменко[3]

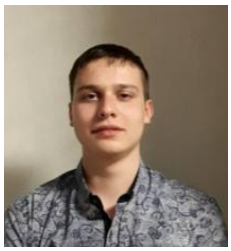
[1]Харківський національний університет імені В.Н. Каразіна, Україна
[2] Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна
[3] Харківський національний університет радіоелектроніки, Україна

БАРАННІК Володимир Вікторович, д.т.н., професор.

Рік та місце народження: 1971 рік, м. Ізюм, Харківська область, Україна.
Освіта: Харківський військовий університет, 1994 рік.
Посада: професор кафедрі штучного інтелекту та програмного забезпечення Харківського національного університету імені В.Н. Каразіна.
Наукові інтереси: технології кодування, штучний інтелект, інформаційна безпека.
Публікації: більше 750 наукових публікацій, серед яких монографії, посібник, навчальні посібники, наукові статті, патенти на винаходи.
E-mail: vvbar.off@gmail.com.
Orcid ID: 0000-0002-2848-4524.

СІДЧЕНКО Сергій Олександрович, к.т.н., с.н.с.

Рік та місце народження: 1972 рік, м. Веймар, Німеччина.
Освіта: Харківський військовий університет, 1994 рік.
Посада: докторант Харківського національного університету Повітряних Сил імені Івана Кожедуба.
Наукові інтереси: технології кодування, інформаційна безпека, інформаційна війна.
Публікації: більше 250 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях, патенти на винаходи.
E-mail: sidserg72@gmail.com.
Orcid ID: 0000-0002-1319-6263.



БАРАННІК Валерій Володимирович

Рік та місце народження: 2000 рік, м. Первомайськ, Миколаївська область, Україна.
Посада:: студент Харківського національного університету радіоелектроніки.
Наукові інтереси: технології цифрової обробки зображень, інформаційна безпека.
Публікації: більше 20 наукових публікацій, серед яких наукові статті, монографії, тези та матеріали доповідей на конференціях.
E-mail: valera462000@gmail.com.
Orcid ID: 0000-0003-3516-5553.

ІГНАТЬЄВ Олександр Олексійович

Рік та місце народження:: 2002 рік, м. Харків, Україна.
Посада:: студент Харківського національного університету радіоелектроніки.
Наукові інтереси: технології цифрової обробки зображень, інформаційна безпека.
Публікації: 5 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях.
E-mail: oleksandr.ignatyev10@gmail.com.
Orcid ID: 0000-0003-1227-6840.

Анотація. *У системах кризового управління потрібне забезпечення конфіденційності переданих відеоданих зі збереженням заданої якості інформації та без зниження її доступності. Однак, існує проблема пов'язана з тим, що забезпечення конфіденційності відеоданих може бути організовано або за рахунок доступності відеоданих при збереженні заданої їх якості, або за рахунок зниження обсягу корисної інформації для підтримки заданої доступності. Розроблено метод скремблювання системи службових складових в криптокомпресійних кодограмах, сформованих за умови відкидання найменшого значущого розряду в значеннях яскравості пікселів в просторі RGB. Відмінність даного методу від відомих полягає в що, перед виконанням скремблюючих перетворень організовується об'єднання службових даних, представлених в зниженому динамічному діапазоні, в 8-бітові об'єднані елементи. На етапі перестановки об'єднаних 8-бітових даних організовується не лише зміна місця розташування значень вихідних 7-бітних елементів службових складових, але також і зміна їх значень. Це дозволяє підвищити криптографічні характеристики відомих перестановочних перетворень. Розроблений метод забезпечує: підвищення доступності відеоданих за рахунок додаткового зменшення обсягу криптокомпресійного представлення зображення; підвищення криптостійкості за рахунок зміни значень елементів системи службових даних, порушення кореляції між елементами та зміни частоти появи пікселів. Скремблюючі перетворення на основі таблиць перестановки, застосовувані до системи службових складових в криптокомпресійних кодограмах, забезпечують стійкість візуальної інформації зображення до помилок в кодограмах, що виникають в каналі зв'язку. Це при тому, що криптокомпресійні кодограми представляють собою стисле представлення вихідних зображень.*

Ключові слова: *криптокомпресійне кодування, захист інформації, скремблювання, шифрування, кодування, перестановка, компресія, конфіденційність, зображення.*

Вступ

У системах кризового управління потрібне забезпечення конфіденційності переданих відеоданих зі збереженням заданої якості інформації та без зниження її доступності.

Однак, існує проблема пов'язана з тим, що забезпечення конфіденційності відеоданих може бути організовано або за рахунок доступності відеоданих при збереженні заданої їх якості, або за рахунок зниження обсягу корисної інформації для підтримки заданої доступності.

Аналіз існуючих підходів щодо забезпечення конфіденційності зображень показав, що найбільш розповсюджені криптографічні методи захисту на основі скремблювання та шифрування даних.

Вони використовуються в наступних підходах:

– застосування криптографічних перетворень до різних представлень відеоданих [1–5];

– на основі поетапного виконання компресійних та криптографічних перетворень [6];

– на основі стеганографічних методів [7–16].

– технологіях візуальної криптографії на основі об'єднання та розсіювання елементів зображень [17–21];

– схемах скремлювання елементів нестиснених зображень [22–27];

– схемах перцептивного шифрування до виконання компресіного перетворення [28–31];

– застосування криптографічних перетворень на різних етапах технологій компресі [32–42].

Методи скремблювання є менш стійкими з позиції захисту інформації. Найбільш часто вони організовуються на основі операцій перестановок, які змінюють місце розташування даних в межах оброблюваних блоків або всього зображення. Однак перестановки не змінюють самих оброблюваних даних. Організація перестановок в межах блоків вихідних даних малої розмірності взагалі не забезпечує конфіденційності зображень. Через психовізуальні особливості сприйняття відеоданих, великі об'єкти в таких скрембльованих зображеннях можуть бути помітні. Для усунення даного недоліку використовуються перестановки для блоків даних більших розмірів аж до розмірів зображень, а також перестановки самих оброблюваних блоків в межах всього кадру та/або між кадрами. Скремблюючі перетворення на основі таблиць перестановки, застосовувані до відкритих відеоданих, підвищують стійкість візуальної інформації зображення до помилок в фрагментах скрембльованих зображення, що виникають в результаті помилок в каналі зв'язку [43].

Однак, використання скремблюючих перетворень в сучасних технологіях компресії нейтралізує даний виграшний ефект. Це пов'язано з тим, що помилки в стислих даних є дуже суттєвими.

Методи шифрування дозволяють забезпечити більш стійкий захист даних. Вони змінюють самі дані не змінюючи їх розташування. Невеликим винятком з позиції зміни місця розташування при блокової обробці даних є байтові та/або бітові перестановки в межах блоку. Однак при обробці даних в блоках або напівблоках шифрування розмірністю від 32 до 256 біт такі перестановки без використання інших криптографічних примітивів є нікчемними, тому що в них бере участь тільки від 4 до 32 байт інформації (8-бітних елементів даних, що обробляються).

Такі перестановки в алгоритмах шифрування призначені для організації лавинного ефекту при розсіюванні і перемішуванні даних. Методи шифрування

критичні до виникнення помилок в зашифрованих даних.

Навіть одинична помилка в блоці зашифрованих даних призводить до його неправильного розшифрування. А в разі використання схем гамування, неправильно розшифрованими можуть виявитися і всі блоки даних, розташовані за помилковим блоком.

Існуючим підходам забезпечення конфіденційності відеоданих характерні наступні проблемні недоліки:

– забезпечення конфіденційності відеоданих без використання технологій компресії призводить до істотного зниження їх доступності;

– забезпечення конфіденційності зображень з використанням технологій компресії після та/або між етапами процесу стиснення даних фактично засноване на поділі функціоналу шифрування і компресії. Це так само призводить до зниження доступності відеоданих;

– в криптографічних перетвореннях відсутні недетерміновані характеристики. Це може вплинути на рівень криптостійкості особливр при використанні скремблюючих перетворень.

Для їх усунення даних проблемних недоліків були розроблені підходи щодо криптокомпресійного кодування зображень, що забезпечують комплексування технологій компресії та шифрування [44–48].

Сформовані криптокомпресійні кодограми зображень складаються з інформаційної та службової складових. Інформаційна складова, яка містить інформацію про вихідні значення елементів в зображенні, являє собою зашифроване представлення, яке неможливо правильно декодувати без наявності службової складової. Службова складова містить інформацію про виявлені структурні характеристики в зображенні.

Вона є ключовим елементом для декодування інформаційної складової. У відритому вигляді з елементів службової складової можна реконструювати образ зображення в зменшеному розмірі.

Тому для забезпечення криптографічної стійкості всієї кріптокомпресійної кодограми потрібно організувати додаткове криптографічне перетворення над елементами службової складової, яке може бути побудовано на основі алгоритмів скремблювання або шифрування даних.

Метою статті є розробка методу скремблювання системи службових складових криптокомпресійних кодограм для забезпечення криптостійкості відеоданих зі збереженням заданої якості інформації без зниження її доступності. Особливість організації криптокомпресійного кодування полягає в тому, що службові складові з одного боку визначають правильну довжину відповідних їм кодів інформаційної складової, а з іншого боку визначають кількість елементів вихідного зображення, які сформували дані коди, і дозволяють правильно декодувати їх значення. Службові складові, що змінені на основі перетворень скремблювання або шифрування даних, в процесі криптокомпресійного декодування не можуть бути правильно зіставлені з кодами інформаційних складових і відповідно є помилковими для них. Крім того, хибні службові складові не дозволяють правильно декодувати зображення.

Причому в процесі криптокомпресійного декодування на основі хибних службових складових помилки накопичуються. Це пов'язано з тим, що хибні службові складові криптокомпресійних кодограм при декодуванні проміжних значень службових складових першого каскаду також формують помилкові значення. Вони в свою чергу неправильно декодують реконструйовані елементи, які не збігаються з вихідними значеннями.

Процес організації криптографічного перетворення службових складових криптокомпресійних кодограм будемо розглядати в загальному вигляді, який залежить від способу представлення даних, що захищаються, та організації їх перетворення без вибору конкретного алгоритму перетворення. Службові складові криптокомпресійних кодограм можуть бути представлені у вихідному динамічному діапазоні та в зниженому динамічному діапазоні за рахунок відкидання молодшого значущого розряду у елементів вихідних зображень в процесі їх криптокомпресійного кодування.

У першому випадку, коли службові складові представлені у вихідному динамічному діапазоні, для зберігання значення яскравості одного елементу виділяється 8 біт (1 байт). У другому випадку для зберігання значення яскравості одного елемента в зниженому динамічному діапазоні потрібно $(8-n_{LSB})$ біт, де n_{LSB} – кількість відкинутих молодших розрядів в елементі зображення. Для забезпечення мінімальної втрати якості реконструкції зображень в криптокомпресійних перетвореннях було запропоновано відкидати один молодший значущий розряд у елементів вихідного зображення. Тому, для зберігання значення яскравості одного елемента службових складових в зниженому динамічному діапазоні виділяється 7 біт.

Основна частина

Розглянемо процес організації скремблюючих перетворень службових складових криптокомпресійних кодограм. Перестановки службових складових можуть організовуватися, як без урахування зміни їх динамічного діапазону, так і з урахуванням цієї зміни. У першому варіанті передбачається, що перестановці піддаються дані в їх вихідному динамічному діапазоні, тобто організовується тільки зміна їх розташування в межах

блоку скремблювання або в межах всіх службових складових.

Так, перестановка службових складових у вихідному динамічному діапазоні передбачає організацію звичайних байтових перестановок. Перестановка службових складових в зниженому динамічному діапазоні передбачає організацію перестановок елементів довжиною ($8-n_{LSB}$) біт.

Для службових складових з одним відкинутим молодшим розрядом організовується перестановка 7-бітних елементів. Така організація перестановки забезпечує розрив кореляційних взаємозв'язків між елементами службових складових (хоча самі елементи не змінюються) і розрив відповідності службових складових з кодами інформаційних складових.

Другий варіант організації скремблюючих перетворень передбачає об'єднання службових даних, представлених в зниженому динамічному діапазоні з довжиною ($8-n_{LSB}$) біт кожний при $n_{LSB}>0$ в 8-бітові об'єднані елементи.

Це пов'язано з тим, що, як правило, дані обробляються і зберігаються в 8-бітовому вигляді. Фактично кожен елемент службової складової містить в собі незаповненими (приймаючі нульові значення) старші розряди, кількість яких дорівнює n_{LSB}.

Так як для забезпечення мінімальної втрати якості реконструкції зображень в криптокомпресійних перетвореннях було запропоновано відкидати один молодший значущий розряд у елементів вихідного зображення, то організацію процесу об'єднання службових даних в зниженому динамічному діапазоні в 8-бітові дані будемо розглядати з позиції обробки 7-бітних даних.

Об'єднані 8-бітові дані в подальшому піддаються байтовим векторним або матричним перестановкам в межах блоку скремблювання або в межах всіх службових складових.

Нехай необхідно сформувати послідовність з 8-бітних даних d_{i_d}, де i_d – порядковий номер в сформованої послідовності, для організації перестановок над ними, $i_d=\overline{1,i_{d_{max}}}$, $i_{d_{max}}$ – максимальний порядковий номер сформованого 8-бітного елемента.

Для цього використовується послідовність 7-бітних службових складових a_{i_a}, де i_a – порядковий номер елементів службових складових, $i_a=\overline{1,i_{a_{max}}}$, $i_{a_{max}}$ – максимальний порядковий номер елемента службових складових. Максимальний порядкового номера $i_{a_{max}}$ може бути визначений за допомогою формули:

$$i_{a_{max}}=\frac{M\cdot N}{m\cdot n}, \quad (1)$$

де M, N – кількість рядків і стовпців в початковому зображенні, відповідно; m, n – кількість рядків і стовпців у сегменті зображення для організації криптокомпресійних кодограм. Останнім буде сформований 8-бітний елемент $d_{i_{d_{max}}}$ з порядковим номером $i_{d_{max}}$, який визначається відповідно до значення максимального порядкового номера $i_{a_{max}}$ (який визначено за допомогою виразу (1)) для службових даних a_{i_a} в зниженому динамічному діапазоні і рівнем зниження динамічного діапазону n_{LSB} на основі формули:

$$i_{d_{max}}=\frac{(8-n_{LSB})\cdot M\cdot N}{8\cdot m\cdot n}=\frac{(8-n_{LSB})}{8}\cdot i_{a_{max}}. \quad (2)$$

При об'єднанні 7-бітних значень службових складових криптокомпресійних кодограм, коли відкидається одні молодший розряд $n_{LSB}=1$, вираз (2) прийме наступний вигляд:

$$i_{d_{max}}=\frac{7\cdot M\cdot N}{8\cdot m\cdot n}=\frac{7}{8}\cdot i_{a_{max}}. \quad (3)$$

Дане значення буде відповідати:

– загальної кількості сформованих 8-бітних елементів, що піддаються подальшому криптографічному перетворенню;

– розмірності необхідної таблиці для організації векторної перестановки або відповідної їй матричної форми;

– загального обсягу службових даних в байтах для оброблюваної колірної площині.

Останній сформований 8-бітний елемент $d_{i_{d_{max}}}$ повинен бути повністю заповненим, тобто відповідно до виразу (3) повинна виконуватися умова:

$$i_{d_{max}}=[\frac{7}{8}\cdot i_{a_{max}}], \quad \frac{7}{8}\cdot i_{a_{max}}=[\frac{7}{8}\cdot i_{a_{max}}]. \quad (4)$$

Якщо умова (4) не виконується, то біти, що залишилися, заповнюються випадковим чином нульовими та/або одиничними бітовими значеннями.

Умова (4) виконується при мінімальному значенні $i_{a_{max}}=8$. У цьому випадку значення $i_{d_{max}}$ на основі виразу (3) дорівнюватиме 7. Умова (4) буде виконуватися для всіх значень $i_{a_{max}}$ кратних восьми.

Відповідно, можна зробити висновок про те, що кожні 7 послідовних 8-бітних об'єднаних даних будуть сформовані з 8 послідовних 7-бітних значень службових складових. Схема об'єднання 7-бітних значень a_{i_a} службових складових криптокомпресійних кодограм в

8-бітові дані для подальшого їх криптографічного перетворення представлена на рис. 1 для перших семи варіантів об'єднання. Надалі вони будуть циклічно повторюватися. На схемі в блоках даних записана змінна a_{i_a}, яка бере участь в об'єднанні, а через кому кількість її розрядів. Об'єднання бітових розрядів може бути організовано на основі математичних операцій ділення та множення значень на 2 або використанні бітових операцій циклічного зсуву вліво shl і вправо shr.

В рамках цієї статті будимо використовувати бітову арифметику. Формування 8-бітних об'єднаних даних d_{i_d} на основі бітових операцій циклічного зсуву вліво shl і вправо shr в поєднанні з операцією бітового складання по модулю 2 з 7-бітних значень службових складових для перших семи варіантів об'єднання, представлених на рис. 1, організовується за допомогою виразів:

$$d_1 = \mathrm{shl}_1 a_1 \oplus \mathrm{shr}_6 a_2, \quad (5)$$

$$d_2 = \mathrm{shl}_2 a_2 \oplus \mathrm{shr}_5 a_3, \quad (6)$$

$$d_3 = \mathrm{shl}_3 a_3 \oplus \mathrm{shr}_4 a_4, \quad (7)$$

$$d_4 = \mathrm{shl}_4 a_4 \oplus \mathrm{shr}_3 a_5, \quad (8)$$

$$d_5 = \mathrm{shl}_5 a_5 \oplus \mathrm{shr}_2 a_6, \quad (9)$$

$$d_6 = \mathrm{shl}_6 a_6 \oplus \mathrm{shr}_1 a_7, \quad (10)$$

$$d_7 = \mathrm{shl}_7 a_7 \oplus a_8. \quad (11)$$

Тут $\oplus$ – бітова операція "виключає АБО" (додавання по модулю 2). Роботу бітових операцій циклічного зсуву вліво shl і вправо shr описує наступний приклад. Число $204 = 11001100_2$ в результаті операцій циклічного зсуву на 2 біта вліво $\mathrm{shl}_2 204$ перетворюється в значення $48 = 00110000_2$.

А результатом операцій циклічного зсуву на 2 біти вправо $\mathrm{shr}_2 204$ буде число $51 = 00110011_2$.

Вирази (5)–(11) для формування 8-бітних об'єднаних даних на основі бітових операцій в загальному випадку приймуть вид:

$$d_{i_d} = \begin{cases} \mathrm{shl}_{i_d - [\frac{i_d}{7}]\cdot 7} a_{i_d + [\frac{i_d}{7}]} \oplus \mathrm{shr}_{7-\left(i_d - [\frac{i_d}{7}]\cdot 7\right)} a_{i_d + [\frac{i_d}{7}]+1}, & [\frac{i_d}{7}] \neq \frac{i_d}{7}; \\ \mathrm{shl}_7 a_{i_d + [\frac{i_d}{7}]-1} \oplus a_{i_d + [\frac{i_d}{7}]}, & [\frac{i_d}{7}] = \frac{i_d}{7}. \end{cases} \quad (12)$$

З аналізу схеми формування 8-бітних об'єднаних даних d_{i_d} з 7-бітних службових складових a_{i_a}, представленої на рис. 1 і описаної виразами (5)–(12), видно, що:

– кожних байт об'єднаних даних d_{i_d} для подальшого криптографічного перетворення складається з бітів, що належать двом 7-бітовим елементів службової складової, що стоять поруч, a_{i_a} і a_{i_a+1};

– у формуванні тільки кожного першого і кожного сьомого 8-бітного об'єднаного елемента d_{i_d} приймають участь всі бітові розряди, відповідно, кожного першого і кожного восьмого 7-бітного елемента a_{i_a} службових складових. У формуванні всіх інших 8-бітних об'єднаних елементів d_{i_d} (а саме, з другого по шостий) беруть участь окремі бітові розряди 7-бітних елементів службової складової, що стоять поруч, a_{i_a} і a_{i_a+1};

– формування кожних 7 послідовних 8-бітових об'єднаних даних d_{i_d}, що використовуються для подальшого криптографічного перетворення, з повністю заповненими бітовими розрядами організовується на основі 8 послідовних елементів a_{i_a} службової складової, з яких використовуються всі бітові значення;

– загальна довжина 7 послідовних 8-бітових об'єднаних даних d_{i_d} з повністю заповненими бітовими розрядами становить 56 біт.

Після об'єднання всіх $i_{a_{max}}$ 7-бітних службових складових a_{i_a} в 8-бітові об'єднані дані d_{i_d}, останні піддаються криптографічному перетворенню на основі векторної або матричної перестановки.

В результаті виконання перестановочного перетворення організовується зміна місця розташування 8-бітних об'єднаних даних d_{i_d}.

А так як вони складаються з бітових значень двох поруч стоять 7-бітних елементів службової складової a_{i_a} і a_{i_a+1}, то дана перестановка фактично призводить до поділу 7-бітних елементів на частини і має свої особливості:

– при формуванні кожного першого і сьомого елемента 8-бітних об'єднаних даних d_{i_d} спостерігаються ситуації, коли всі розряди 7-бітного елемента службових складових a_{i_a} потрапляють в один 8-бітний елемент d_{i_d} (це кожен перший і кожен восьмий 7-бітний елемент a_{i_a} службових складових при розбитті їх в групи по 8 елементів). Перестановка таких даних призводить тільки до зміни їх розташування;

– розряди кожного другого - сьомого 7-бітного елемента a_{i_a} службових складових з груп по 8 елементів, що стоять поруч, потрапляють в два різних сусідніх 8-бітних об'єднаних елемента d_{i_d}.

Саме ці 7-бітові елементи a_{i_a} службових складових за рахунок зміни місця розташування 8-бітних об'єднаних даних d_{i_d} поділяються і координати їх окремих бітових підпослідовностей віддаляються одна від одної.

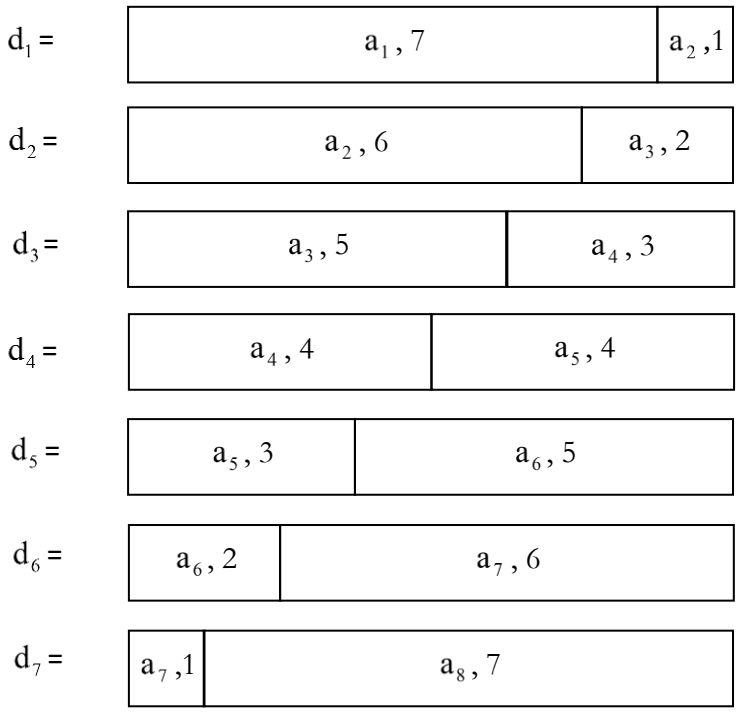


Рис. 1. Схема об'єднання 7-бітних значень службових складових в 8-бітові об'єднані дані

При цьому положення окремих розрядів 7-бітних елементів a_{i_a} службових складових всередині 8-бітних об'єднаних даних d_{i_d} не змінюється. Приклади поділу 7-бітних елементів a_{i_a} службових складових за рахунок зміни місця розташування 8-бітних об'єднаних даних d_{i_d} в процесі векторної та матричної перестановки представлені на рис. 2.

З позиції криптографії даний підхід до об'єднання 7-бітних елементів в 8-бітові даний з подальшою організацією байтової перестановки виконує функції розсіювання і змішування службових складових в криптокомпресійних кодограмах.

На етапі реконструкції 7-бітних елементів $a_{i_a}^{\bullet}$ службових складових без організації зворотного скремблюючого перетворення або його організація на основі не автентичної перестановки відбувається не тільки не правильне відновлення розташування 8-бітних даних $d_{i_d}^{\bullet} \neq d_{i_d}$, але і самі елементи службових складових не можуть бути відновлені, тобто $a_{i_a}^{\bullet} \neq a_{i_a}$.

Даний варіант організації скремблювання службових складових криптокомпресійних кодограм на основі перестановки елементів за умови об'єднання 7-бітних службових даних в 8-бітові об'єднані представлення є більш виграшним, ніж використання варіанту без об'єднання даних.

Виграш полягає в наступному:

– забезпечується підвищення криптостійкості скремльованих службових складових за рахунок змішування і розсіювання даних на етапі їх об'єднання в 8-бітові представлення з подальшою організацією байтової векторної або матричної перестановки. На відміну від стандартного підходу, організуючого зміну місця розташування елементів, забезпечується додаткове зміна їх значень. Причому, при використанні стандартного підходу на основі перестановок елементів у вихідному динамічному діапазоні криптостійкість криптокомпресійних кодограм визначається тільки криптостійкістю використовуваного скремблюючого перетворення (не вище даного перетворення). Другий варіант, коли перестановка організується спільно з об'єднанням 7-бітних елементів в 8-бітові представлення, фактично забезпечується підвищення криптостійкості;

– для організації скремблюючих перетворень в межах всієї множини елементів службових складових потрібно формування таблиць перестановки меншої розмірності.

Це призведе до підвищення оперативності формування таблиць перестановки при збереженні їх криптостійкості (ключові параметри і алгоритм формування таблиць перестановки залишаються незмінними), а так само підвищиться оперативність виконання самого перестановочного перетворення за рахунок обробки меншої кількості даних.

Все це також сприяє підвищенню доступності відеоінформації.

Розмірність матриці перестановок для випадку її організації для елементів у вихідному динамічному діапазоні перевершує варіант її організації для 7-бітних службових складових, об'єднаних в 8-бітові дані, на 12,5%.

Реконструкція 7-бітних елементів $a_{i_a}^{\bullet}$ службових складових з об'єднаних 8-бітних даних $d_{i_d}^{\bullet}$ (які можуть бути, як автентифікованими так і ні) організовується на основі зворотних перетворень з використанням операцій бітової арифметики в загальному випадку за допомогою виразу:

$$a_{i_a}^{\bullet} = \begin{cases} \mathrm{shl}_1 d_{[\frac{i_a}{8}]\cdot 7+1}^{\bullet}, & [\frac{i_a}{8}] \neq \frac{i_a}{8}, i_a - [\frac{i_a}{8}]\cdot 8 = 1; \\ \mathrm{shl}_{8-\left(i_a-[\frac{i_a}{8}]\cdot 8\right)} d_{[\frac{i_a}{8}]\cdot 7+(i_a-[\frac{i_a}{7}]\cdot 8)-1}^{\bullet} \oplus \mathrm{shr}_{i_a-[\frac{i_a}{8}]\cdot 8} d_{[\frac{i_a}{8}]\cdot 7+(i_a-[\frac{i_a}{7}]\cdot 8)}^{\bullet}, & [\frac{i_a}{8}] \neq \frac{i_a}{8}, i_a - [\frac{i_a}{8}]\cdot 8 \neq 1; \\ \mathrm{shr}_1\left(\mathrm{shl}_1 d_{[\frac{i_a}{8}]\cdot 7}^{\bullet}\right), & [\frac{i_a}{8}] = \frac{i_a}{8}. \end{cases}$$

У разі, якщо на етапі реконструкції 7-бітних елементів $a_{i_a}^{\bullet}$ службових складових була організована автентифікована схема дескремблюючого перетворення (використовувався автентифікований ключ) і об'єднані 8-бітові дані $d_{i_d}^{\bullet}$ не піддавалися модифікації, тобто $d_{i_d}^{\bullet} = d_{i_d}$, то реконструйовані значення $a_{i_a}^{\bullet}$ службових складових співпадуть з вихідними a_{i_a}, тобто буде виконуватися рівність $a_{i_a}^{\bullet} = a_{i_a}$.

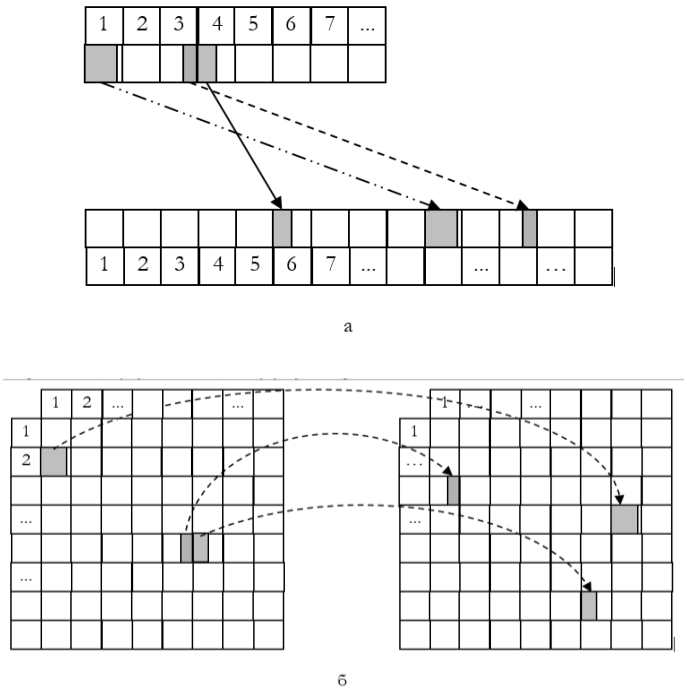


Рис. 2. Приклади поділу елементів службових складових за рахунок зміни місця розташування об'єднаних даних в процесі перестановки: а – векторна перестановка, б – матрична перестановка

Експериментальна частина

Були проведені експериментальні дослідження щодо оцінки якості забезпечення конфіденційності в схемі криптокомпресійного кодування зображень в просторі RGB за умови зниження динамічного діапазону вихідних значень за рахунок відкидання одного молодшого значущого розряду з подальшим скремблюванням службових складових, об'єднаних в 8-бітові дані.

Оцінка проводилася на основі порівняння вихідних зображень з реконструйованими зображеннями, відновленими з криптокомпресійних кодограм зі скремльованими службовими складовими.

Для прикладу в статті представлені результати обробки тільки декількох тестових зображень різного ступеня насиченості.

При цьому отримані результати характерні для більшості з оброблюваних відеоданих. Для оцінки якості використовувалися такі підходи:

– візуальна оцінка якості вихідних та відповідних їм скрембльованих зображень;

– кількісна оцінка якості обробки зображень за допомогою показників якості середньоквадратичного відхилення RSME (mean squared error), пікового відношення сигналу до шуму PSNR (Peak Signal-to-Noise Ratio) та коефіцієнта кореляції;

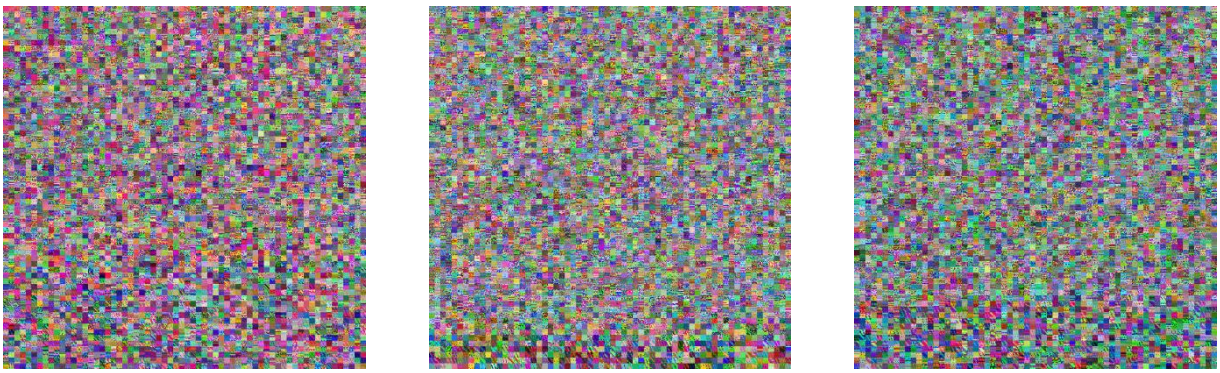
– оцінка кількості пікселів, що змінюються, NPCR (Number of Changing Pixel Rate), яка найбільш часто використовується для оцінки якості шифрування зображень;

– оцінка якості розсіювання та перемішування пікселів в скрембльованих даних за допомогою побудови гістограм кореляції між елементами в скрембльованих зображеннях та гістограм розподілу елементів в скрембльованих зображеннях;

– оцінка можливості додаткової компресії даних на основі використання архіваторів ZIP і RAR.

В експерименті в якості базового скремблюючого перетворення було використано логістичне відображення [49].

Результати оцінки якості забезпечення конфіденційності відеоданих за основі використання запропонованих рішень представлені на рис. 3, 4 і в табл. 1.



Lena Baboon Зона аеропорту

Рис. 3. Приклади візуалізації скрембльованих зображень

Таблиця 1

Результати оцінки якості скрембльованих зображень

Тестове зображення	Показники якості обробки			
	RSME	PSNR, dB	коефіцієнт кореляції	NPCR, %
Baboon	88,94	9,15	-0,0030	99,5832
Lena	87,02	9,34	0,0760	99,5519
Зона аеропорту	82,20	9,83	0,0029	99,5518

З аналізу отриманих результатів можна зробити наступні висновки:

– візуальна оцінка якості зображень (рис. 3) показує повне їх руйнування. Скрембльовані представлення різних зображень практично стали схожі один на одного. Домінуючий фон окремих вихідних зображень повністю зруйнований;

– значення показників RSME, PSNR і коефіцієнта кореляції між скрембльованими та вихідними зображеннями (табл. 1) повністю підтверджують дані візуальної оцінки про повне руйнування відеоданих.

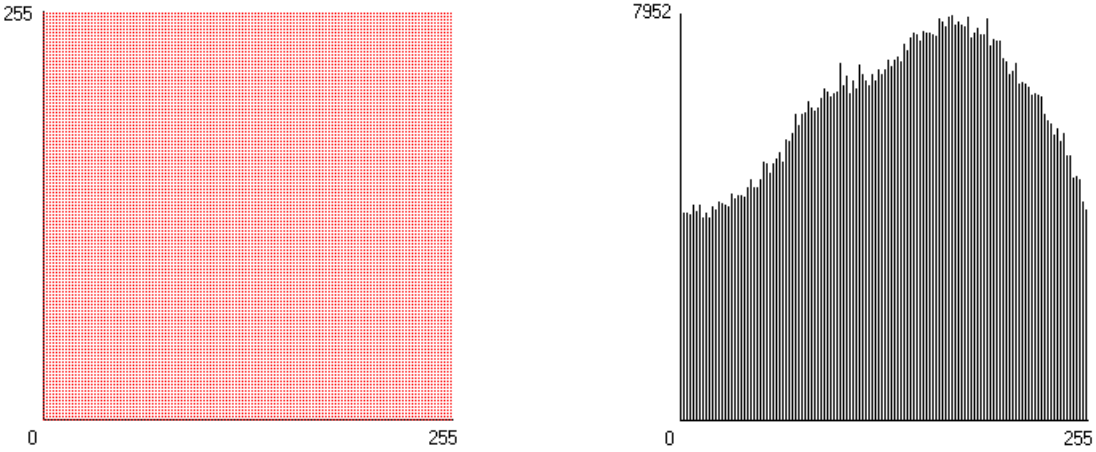
Для всіх типів зображень значення RSME знаходиться вище 80, PSNR – нижче 10 dB. Значення коефіцієнтів кореляції для більшості зображень знаходиться в

районі 0, хоча для деяких відеоданих значення коефіцієнта кореляції можуть спостерігатися в районі до 0,1;

– кількості пікселів, що змінюється, NPCR (табл. 1) для всіх зображень знаходиться вище теоретичного порогового значення 99.5341% [50 – 52], що свідчить про високу стійкість зашифрованих даних до диференціальних атак;

– гістограми кореляції між елементами для різних зображень збігаються незалежно від їх вмісту (рис. 4,а). На гістограмах сформувалося зображення у вигляді квадрата, що істотно змінило гістограми вихідних відеоданих. Через те що дані реконструюються в зниженому діапазоні за рахунок відкидання молодшого розряду, як і в вихідних відеоданих, на гістограмі на рис. 4,а в квадраті пікселі розташовані через один у вертикальному і горизонтальному напрямках. Гістограма у вигляді квадрата свідчить про повністю зруйновану кореляція між сусідніми елементами;

– гістограми розподілу елементів для різних зображень щодо вихідних відеоданих сильно змінилися, відбулося значне вирівнювання кількості елементів (рис. 4,б). Через те що дані обробляються з урахуванням зниження їх динамічного діапазону, на гістограмах відліки розташовуються через один. Фактично присутні тільки елементи з парними значеннями. На гістограмах спостерігаються зміни кількості елементів і відсутні варіанти, коли немає якогось парного значення яскравості або кількість даних значень є малою.



а б

Рис. 4. Приклад гістограм оцінки вмісту скрембльованих тестового зображення:
а – кореляція між елементами; б – розподіл елементів

На гістограмах розподілу елементів не організовується повного вирівнювання їх кількості, з одного боку, через те, що в процесі скремблювання об'єднаних 8-бітних даних змінюються значення тільки кожних шості 7-бітних значень службових складових з восьми, тоді як два значення (перше і восьме) залишаються без зміни.

З іншого боку, в процесі скремблювання не використовувалися спеціальні перетворення, що усувають надмірність. Оцінка додаткової компресії криптокомпресійоних кодограм відеоданих за допомогою архіваторів ZIP і RAR показав, що розміри кодограм додатково не зменшуються.

Для більшості даних навпаки спостерігається незначне збільшення їх обсягу за рахунок формування архіваторами ZIP і RAR своєї службової інформації на початку сформованого архіву. Це свідчить про відсутність надмірності в сформованих криптокомпресійоних кодограмах та про усунення кореляції між елементами.

Відкидання одного молодшого незначущого розряду, що організоване в схемі криптокомпресійного перетворення без втрати якості інформації, з одного боку, призводить до зниження якості реконструйованих даних.

Хоча, данє зниження якості є незначним.

Для всіх зображення значення показника RSME знаходиться на рівні 0,71, PSNR – вище 51 dB, а коефіцієнт кореляції становить 0,9999. З іншого боку забезпечується:

– підвищення доступності відеоданих за рахунок додаткового зменшення обсягу криптокомпресійного представлення зображення;

– підвищення криптостійкості за рахунок зміни значень елементів системи службових даних, порушення кореляції між елементами та зміни частоти появи пікселів.

Висновки

Наукова новизна отриманих результатів.

Розроблено метод скремблювання системи службових складових в криптокомпресійних кодограмах, сформованих за умови відкидання найменшого значущого розряду в значеннях яскравості пікселів в просторі RGB. Відмінність даного методу від відомих полягає в що, перед виконанням скремблюючих перетворень організовується об'єднання службових даних, представлених в зниженому динамічному діапазоні, в 8-бітові об'єднані елементи.

На етапі перестановки об'єднаних 8-бітових даних організовується не лише зміна місця розташування значень вихідних 7-бітних елементів службових складових, але також і зміна їх значень. Це дозволяє підвищити криптографічні характеристики відомих перестановочних перетворень. Розроблений метод забезпечує:

– підвищення доступності відеоданих за рахунок додаткового зменшення обсягу криптокомпресійного представлення зображення;

– підвищення криптостійкості за рахунок зміни значень елементів системи службових даних, порушення кореляції між елементами та зміни частоти появи пікселів.

Практичне значення отриманих результатів. Створена програмна реалізація методу скремблювання системи службових складових в криптокомпресійних кодограмах, яка забезпечує:

– формування захищених криптокомпресійних кодових конструкцій зі скрембльованими службовими складовими. Реконструйовані неавтентифікованими користувачаими зображення є повністю зруйнованими і все скрембльовані зображення візуально не відрізняються одне від одного;

– для всіх скрембльованих зображень забезпечується значне зниження їх якості в порівнянні з вихідними відеоданими. Показники якості для таких зображень приймають наступні значення: RSME знаходиться вище 80, PSNR – нижче 10 dB. Значення коефіцієнтів кореляції для більшості зображень знаходиться в районі 0, хоча для деяких відеоданих значення коефіцієнта кореляції можуть спостерігатися в районі до 0,1. Кількість пікселів, що змінюється, NPCR для всіх зображень знаходиться вище теоретичного порогового значення 99.5341%.

Скремблюючі перетворення на основі таблиць перестановки, застосовувані до системи службових складових в криптокомпресійних кодограмах, забезпечують стійкість візуальної інформації зображення до помилок в кодограмах, що виникають в каналі зв'язку. Це при тому, що криптокомпресійні кодограми представляють собою стисле представлення вихідних зображень.

Література

[1] Schneier B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York City, United States: Wiley, 2015. – 784 p.

[2] Announcing the ADVANCED ENCRYPTION STANDARD (AES*) // Federal Information Processing Standards Publication* [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[3] DSTU 7624:2014: *Information Technology. Cryptographic protection of information. Symmetric block transformation algorithm.* Order of the Ministry of Economic Development of Ukraine № 1484, 2014.

[4] DSTU GOST 28147:2009: *Information processing system. Cryptographic protection. Cryptographic transformation algorithm* GOST 28147-89, 2008.

[5] Rivest R.L., Shamir A., Adleman L.M. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, Vol. 2, Iss. 21, 1978. - pp. 120–126.

[6] Sharma R., Bollavarapu S. Data Security using Compression and Cryptography Techniques. *International Journal of Computer Applications*, Vol. 117, No. 14, 2015. - pp. 15-18.

[7] Barannik, D. Stegano-Compression Coding in a Non-Equalible Positional Base // *IEEE 2 nd International Conference on Advanced Trends in Information Theory (ATIT 2020)*, 2020, pp. 83-86.

[8] Barannik V., Barannik D., Fustii V., Parkhomenko M. Evaluation of Effectiveness of Masking Methods of Aerial Photographs // *3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019. - pp. 415-418.

[9] Barannik V., Barannik N., Ryabukha Yu., Barannik D. Indirect Steganographic Embedding Method Based On Modifications of The Basis of the Polyadic System // *15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020)*, 2020. - pp. 699-702.

[10] Barannik V., Barannik, V.: Binomial-Polyadic Binary Data Encoding by Quantity of Series of Ones // *15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020)*, 2020. - pp. 775-780.

[11] Barannik V.V., Ryabukha Yu. N., Tverdokhleb V.V., Barannik D.V. Methodological basis for constructing a method for compressing of transformants bit representation, based on non-equilibrium positional encoding // *2nd International Conference on Advanced Information and Communication Technologies (AICT)*, 2017. - pp.188-192.

[12] Barannik V., Krasnoruckiy A., Hahanova A. The positional structural-weight coding of the binary view of transformants // *East-West Design & Test Symposium (EWDTS)*, 2013. – pp 1-4.

[13] Barannik V.V., Ryabukha Yu.N., Kulitsa O.S. The method for improving security of the remote video information resource on the basis of intellectual processing of video frames in the telecommunication systems. *Telecommunications and Radio Engineering*, Vol. 76, No 9, 2017. - pp. 785-797.

[14] Barannik V., Barannik V., Havrylov D., Sorokun A. Development Second and Third Phase of the Selective Frame Processing Method // *3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019. - pp. 54-57.

[15] Barannik V., Shulgin S. The method of increasing accessibility of the dynamic video information resource // *13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, 2016. - pp. 621-623.

[16] Barannik V., Tarasenko D. Method coding efficiency segments for information technology processing video // *4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, 2017. - pp. 551-555.

[17] Chen Ch.-Ch., Wu W.-J. A secure Boolean-based multi-secret image sharing scheme. *Journal of Systems and Software*, Vol. 92, 2014. - pp. 107-114.

[18] Chen T.-H., Wu Ch.-S. Efficient multi-secret image sharing based on Boolean operation. *Signal Processing*, Vol. 91, Iss. 1, 2011. - pp. 90-97.

[19] Deshmukh M., Nain N., Ahmed M. An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic // *IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, 2016. - pp. 690-697.

[20] Naor M., Shamir A. Visual Cryptography. *Advances in Cryptology – EUROCRYPT'94. Lecture Notes in Computer Science*, Vol. 950, 1995. - pp. 1-12.

[21] Yang Ch.-N., Chen Ch.-H., Cai, S.-R. Enhanced Boolean-based multi secret image sharing scheme. *Journal of Systems and Software*, Vol. 116, 2016. - pp. 22-34.

[22] Barannik V., Babenko Yu., Kulitsa O., Barannik, V., Khimenko A., Matviichuk-Yudina, O. Significant Microsegment Transformants Encoding Method to Increase the Availability of Video Information Resource // *IEEE 2 nd International Conference on Advanced Trends in Information Theory (ATIT 2020)*, 2020, - pp. 52 – 56.

[23] Ramakrishnan S. *Cryptographic and Information Security Approaches for Images and Videos.* CRC Press, 2018. - 962 p.

[24] Tsai Ch.-L., Chen Ch.-J., Hsu W.-L. Multi-morphological image data hiding based on the application of Rubik's cubic algorithm // *IEEE International Carnahan Conference on Security Technology (ICCST0),* 2012. - pp. 135-139.

[25] Wong K.-W. Image encryption using chaotic maps. *Intelligent Computing Based on Chaos*, Vol. 184, 2009. - pp. 333–354.

[26] Wu Yu., Agaian S., Noonan J. Sudoku Associated Two Dimensional Bijections for Image Scrambling // *IEEE Transactions on multimedia* [Електронний ресурс]. Режим доступу: arXiv preprint. arXiv:1207.5856v1.

[27] Zhou Y., Panetta K., Agaian S., Chen C.L.P. Image encryption using P-Fibonacci transform and decomposition. *Optics Communications*, Vol. 285, Iss. 5, 2012. - pp. 594-608.

[28] Kurihara K., Shiota S., Kiya H. An encryption-then-compression system for JPEG standard // *Picture Coding Symposium (PCS)*, 2015. - pp. 119–123.

[29] Kurihara K., Watanabe O., Kiya H. An encryption-then-compression system for JPEG XR standard // *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, 2016. - pp. 1–5.

[30] Watanabe O., Uchida A., Fukuhara T., Kiya H. An Encryption-then-Compression system for JPEG 2000 standard // *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2015. - pp. 1226–1230.

[31] Zhou J., Liu X., Au O. C., Tang Y. Y. Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation. *IEEE Transactions on Information Forensics and Security*, Vol. 9, Iss. 1, 2014. - pp. 39–50.

[32] Auer S., Bliem A., Engel. D., Uhl. A., Unterweger. A. Bitstream-based JPEG Encryption in Real-time. *International Journal of Digital Crime and Forensics*, 2013. – pp. 1-14.

[33] Dufaux F., Ebrahimi T. Toward a Secure JPEG. *Applications of Digital Image Processing* XXIX, Vol. 6312, 2006.

[34] Honda T., Murakami Y., Yanagihara Y., Kumaki T., Fujino T. Hierarchical image-scrambling method with scramble-level controllability for privacy protection // *IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2013. - pp. 1371-1374.

[35] *Information technology – JPEG 2000 image coding system: Secure JPEG 2000*. International Standard ISO/IEC 15444-8; ITU-T Recommendation T.807, 2007. - 108 p.

[36] Ji Sh., Tong X., Zhang M. *Image encryption schemes for JPEG and GIF formats based on 3D baker with compound chaotic sequence generator* [Електронний ресурс]. Режим доступу: arXiv preprint. arXiv: 1208.0999.

[37] Kobayashi H., Kiya H. Bitstream-Based JPEG Image Encryption with File-Size Preserving //*IEEE 7th Global Conference on Consumer Electronics*, 2018. - pp. 1-8.

[38] Minemura K., Moayed Z., Wong K., Qi, X., Tanaka, K. JPEG image scrambling without expansion in bitstream size // *19th IEEE International Conference on Image Processing*, 2012. - pp. 261-264.

[39] Phatak A. A Non-format Compliant Scalable RSA-based JPEG Encryption Algorithm. *International Journal of Image, Graphics and Signal Processing*, Vol. 8, No. 6, 2016. - pp. 64-71.

[40] Wong K., Tanaka K. DCT based scalable scrambling method with reversible data hiding functionality // *4th International Symposium on Communications, Control and Signal Processing (ISCCSP)*, 2010. – pp 1-4.

[41] Yang Y., Zhu B.B., Li S., Yu N. Efficient and Syntax-Compliant JPEG 2000 Encryption Preserving Original Fine Granularity of Scalability. *EURASIP Journal on Information Security*, Vol. 2007, Article ID 56365, 2008. – pp. 1-13.

[42] Yuan L., Korshunov. P., Ebrahimi T. Secure JPEG Scrambling enabling Privacy in Photo Sharing //

11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG), 2015. – pp. 1-6.

[43] Gschwandtner M., Uhl A., Wild P. Transmission error and compression robustness of 2D chaotic map image encryption schemes. *EURASIP Journal on Information Security*, 2007. – pp. 1-16.

[44] Баранник В., Сидченко С., Баранник Д., Баранник В. Оценка влияния недетерминированных характеристик на эффективность криптокомпрессионного кодирования изображений в дифференцированном базисе. *Безпека інформації*, Том 26, № 3, 2020. – С. 168-180.

[45] Баранник В.В., Сидченко С.А., Баранник Д.В. Метод криптокомпрессионного представления изображений на основе двухкаскадного обобщенного позиционного кодирования в базисе по верхним границам. *Радиоэлектроника и информатика*. № 1(76), 2017. - С. 22 – 27.

[46] Barannik V.V., Tupitsya I.M., Sidchenko S.A., Tarnopolov R.V. The Method of Crypto-Semantic Presentation of Images Based on the Floating Scheme in the Basis of the Upper Boundaries // 2th International Scientific-Practical Conference *Problems of Infocommunications. Science and Technology* (PIC S&T'2015), 2015. - pp. 248 – 250.

[47] Сідченко С.О., Бараннік Д.В. Метод криптосемантичного представлення зображень на основі плаваючої схеми системи поліадичного кодування в диференціальному базисі. *Наукоємні технології*. № 1 (33), 2017. – С. 46-53.

[48] Alimpiev A.N., Barannik V.V., Sidchenko, S.A. The method of cryptocompression presentation of videoinformation resources in a generalized structurally positioned space. *Telecommunications and Radio Engineering*, Vol. 76, No 6, 2017. – pp. 521-534.

[49] Barannik V., Sidchenko S., Barannik D. Technology for Protecting Video Information Resources in the Info-Communication Space // *2nd IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, 2020. – pp. 415-418.

[50] Barannik V., Sidchenko S., Barannik N., Barannik V. Development of the method for encoding service data in cryptocompression image representation systems. *Eastern-European Journal of Enterprise Technologies*, Vol. 3, № 9 (111), 2021. – pp. 112-124.

[51] May R. Simple mathematical models with very complicated dynamics. *Nature*, Vol. 261 (5560), 1976. – pp. 459–467.

[52] Y. Wu, J.P. Noonan, S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption. *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, April Edition, 2011. – pp. 31–38.

УДК 621.327:681.5

Баранник В.В, Сидченко С.А., Баранник В.В., Игнатьев А.А. Метод скремблирования системы служебных составляющих криптокомпрессионных кодограмм

Аннотация. *В системах кризисного управления требуется обеспечение конфиденциальности передаваемых видеоданных с сохранением заданного качества информации без снижения ее доступности. Однако, существует проблема связанная с тем, что обеспечение конфиденциальности видеоданных может быть организовано либо за счет увеличения временных затрат на их обработку и доставку при сохранении заданного качества видеоданных, либо за счет снижения объема полезной информации для поддержания заданной доступности. Разработан метод скремблирования системы служебных составляющих в криптокомпрессионных кодограммах, сформированных при условии отбрасывания наименьшего значащего разряда в яркостных значениях пикселей в пространстве RGB. Отличие данного метода от известных заключается в что, перед выполнением скремблирующих преобразований организуется объединение служебных данных, представленных в пониженном динамическом диапазоне, в 8-битные объединенные элементы. На этапе перестановки объединенных 8-битных данных организуется не только изменение местоположения значений исходных 7-битных элементов служебных составляющих, но также и изменение их значений. Это позволяет повысить криптографические характеристики известных перестановочных преобразований. Разработанный метод обеспечивает: повышение доступности видеоданных за счет дополнительного уменьшения объема криптокомпрессионного представления изображения; повышение криптостойкости за счет изменения значений элементов системы служебных данных, нарушения корреляции между элементами и изменения частоты появления точек. Скремблирующие преобразования на основе таблиц перестановки, применяемые к системе служебных составляющих в криптокомпрессионных кодограммах, обеспечивают устойчивость визуальной информации изображения к ошибкам в кодограммах, возникающим в канале связи. Это при том, криптокомпрессионные кодограммах представляют собой сжатое представление исходных изображений.*

Ключевые слова: *криптокомпресионное кодирования, защита информации, скремблирование, шифрование, кодирование, перестановка, компрессия, конфиденциальность, изображение.*

Barannik V., Sidchenko S., Barannik V., Ignatyev O. The method for scrambling the system of service components in the cryptocompression codograms

Annotation. *Crisis management systems require the confidentiality of transmitted video data while maintaining the specified quality of information and without reducing its availability. However, there is a problem associated with the fact that ensuring the confidentiality of video data can be organized either by the availability of video data while maintaining a given quality, or by reducing the amount of useful information to maintain a given availability. The method for scrambling a system of service components in the cryptocompression codograms, formed under the condition of*

discarding the least significant bit in the values of pixel brightness in RGB space, has been developed. The difference between this method and the known ones is that, before performing scrambling transformations, the integration of service components in a reduced dynamic range into 8-bit combined elements is organized. At the stage of permutation of the combined 8-bit data, not only the change of the location of the values of the original 7-bit elements of the service components is organized, but also the change of their values. This improves the cryptographic characteristics of the known permutation transformations. The developed method provides: increase of availability of video data due to additional reduction of volume of cryptocompression image presentation; increasing cryptographic stability by changing the values of the elements of the system of service components, breaking the correlation between the elements and changing the frequency of pixels. Scrambling transformations based on permutation tables applied to the system of service components in cryptocompression codograms, ensure the stability of the visual image information to errors in codograms that arise in the communication channel. Moreover, cryptocompression codograms are a compressed representation of the original images.
Key words: *cryptocompression coding, information protection, scrambling, encryption, encoding, permutation, compression, confidentiality, image.*

Бараннік Володимир Вікторович, д.техн.,наук, професор, професор кафедри штучного інтелекту і програмування, Харківський національний університет імені В.Н. Каразіна.
Баранник Владимир Викторович, д.техн.наук, профессор, профессор кафедры искусственного интеллекта и программирования, Харьковский национальный университет имени В.Н. Каразина.
Volodymyr V. Barannik, Doctor of Technical Sciences, Professor, Professor Department, V.N. Karazin Kharkiv National University.

Сідченко Сергій Олександрович, к. техн. наук, старший науковий співробітник, докторант, Харківський національний університет Повітряних Сил імені І. Кожедуба.
Сидченко Сергей Александрович, к. техн. наук, старший научный сотрудник, докторант Харьковский национальный университет Воздушных Сил шимени И. Кожедуба.
Serhii Sidchenko, PhD, Senior Scientific Researcher, Doctoral Student, Ivan Kozhedub Kharkiv National Air Force University.

Бараннік Валерій Володимирович, студент, Харківський національний університет радіоелектроніки.
Баранник Валерий Владимирович, студент, Харьковский национальный университет радиоэлектроники.
Valery Barannik, student, Kharkov National University of Radio Electronics.

Ігнатьєв Олександр Олексійович, студент Харківського національного університету радіоелектроніки.
Игнатьев Александр Алексеевич, студент Харьковского национального университета радиоэлектроники.
Ignatyev Oleksandr, student, Kharkov National University of Radio Electronics, Kharkiv.

Отримано 26 *липня 2021 року,* затверджено редколегією *27 серпня 2021 року*

DOI: 10.18372/2225-5036.27.16003

ДОСЛІДЖЕННЯ ТА ТЕСТУВАННЯ ЛЕГКОВАГОВИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

Світлана Поперешняк, Олексій Райчев

Київський національний університет імені Тараса Шевченка, Україна

Поперешняк Світлана Володимирівна, к.ф.-м.н., доцент.
Рік та місце народження: 1980 рік, м. Кіровоград, Україна.
Освіта: Кіровоградський державний педагогічний університет імені Володимира Винниченка, 2002 рік.
Посада: доцент кафедри програмних систем і технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
Наукові інтереси: програмна інженерія, автоматизація процесів виробництва, інформаційні технології, захист інформації, використання багатовимірних статистик для тестування бітової послідовності на випадковість.
Публікації: більше 100 наукових публікацій, серед яких навчальні посібники, наукові статті, матеріали та тези доповідей на конференціях.
E-mail: spopereshnyak@gmail.com.
Orcid ID: 0000-0002-0531-9809.

Райчев Олексій Олегович, магістр
Рік та місце народження: 2000 рік, м. Київ, Україна.
Освіта: Київський національний університет імені Тараса Шевченка, 2021 рік.
Посада: магістр кафедри програмних систем і технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
Наукові інтереси: програмна інженерія, статистичні методи, інформаційні технології, захист інформації.
Публікації: 6 наукових публікацій.
E-mail: mileenocktopus@gmail.com.
Orcid ID: 0000-0002-4085-5711.

Анотація. *Аналіз випадкових послідовностей та генераторів випадкових чисел є доволі специфічною задачею, але для її вирішення може бути використаний один або декілька з численних пакетів тестів. Однак, виконаний аналіз вказує на те, що існуючі тести мають низку недоліків, вирішення яких може зменшити передумови до тестування та покращити точність отриманих результатів. Робота присвячена доволі актуальній задачі – дослідженню генераторів випадкових чисел, які працюють на пристроях з обмеженими ресурсами, та послідовностей невеликої довжини на випадковість. В роботі було розглянуто побудову фізичної моделі легковагового генератора псевдовипадкових чисел. Використання багатовимірних статистик як основи для випробувань, дозволяє краще дослідити послідовність на випадковість, за рахунок оцінки одночасно декількох характеристик послідовності. Тести багатовимірних статистик засновані на дослідженні входжень шаблонів в послідовність і допомагають виявляти приховані залежності між даними та неякісні генератори. Головною перевагою цих тестів є їх ефективність на послідовностях короткої довжини, тому вони вирішують одну з проблем існуючих тестів, полегшуючи передумови до випробувань. Фізична модель IoT генератора представлена в роботі, на своєму прикладі надає широкий огляд факторів та обмежень, що виникають під час проектування генераторів. Процес тестування та оптимізації генератора з використанням тестів багатовимірних статистик ілюструє придатність пакету програм до використання і його інтегральну роль в створенні якісного генератора випадкових чисел, в особливості для використання в IoT пристроях. Програмний продукт, що було створено в цій роботі може використовуватися для вирішення широкого спектру задач, як уже і було неодноразово зазначено. Одною з найважливіших, та дійсно тою, що може отримати неоціненну користь сферою застосування є криптографія.*

Ключові слова: *легковаговий генератор псевдовипадкових чисел, тестування, багатовимірна статистика, інтернет речей, криптографія.*

Вступ

Генератор псевдовипадкових чисел (ГПВЧ) - це механізм генерації випадкових чисел у комп'ютері. Його називають псевдовипадковим, оскільки отримати справжнє випадкове число за допомогою комп'ютера дуже важко і дорого.

Теоретично справжнє випадкове число можна отримати з таких джерел ентропії [1]:

- навколишній шум;
- радіоактивний розпад;
- шуми струмів в електричних ланцюгах;
- вимірювання реакції користувача (рух миші) тощо.

Інтернет речей (IoT) широко застосовується багатьма галузями для величезної кількості програм [2]. За останнє десятиліття кількість пристроїв IoT зросла в геометричній прогресії [3], і очікується, що вона зросте ще більше.

Наприклад, в інтелектуальній логістиці, де піддони вбудовані в розумні датчики для аналітичних цілей (виявляють, передбачають і запобігають різним подіям, пов'язаним з логістикою).

У розумній логістиці існує складний ланцюжок зацікавлених сторін, для яких безпека та конфіденційність є ключовими питаннями.

Отже, дані, генеровані цими розумними датчиками, які є обмеженими, та повинні бути захищеними. Централізоване управління цими датчиками є надзвичайно складним, тому потреба у розподіленому механізмі безпеки зростає [4].

У розподіленому механізмі кожен пристрій здатний генерувати власні випадкові числа без необхідності конфігурації центральної сторони або вручну.

Аналіз існуючих досліджень

В оглядовій літературі запропоновано кілька легковагових криптографічних примітивів для забезпечення безпеки пристроїв, обмежених ресурсами. Розглянемо криптографічно захищені конструкції генераторів псевдовипадкових чисел (ГПВЧ) для пристроїв, обмежених ресурсами. У роботі [5] автори розробили та впровадили істинний (справжній) генератор псевдовипадкових чисел (СГВЧ), криптографічний генератор псевдовипадкових чисел, який використовує отримані бітові помилки як джерело випадковості у вузлах бездротових датчиків.

У роботі [6] автори представили вдосконалену версію СГВЧ, запропоновану в роботі [7], яка використовує вимірювання, отримані від бездротових вузлів датчиків, як джерела фізичної випадковості. Їх метод використовує розподілений алгоритм виборів лідерів для вибору випадкового джерела даних. Крім того, була оцінена надійність алгоритму СГВЧ проти кількох атак.

ГПВЧ для недорогих інтелектуальних пристроїв, таких як вузли датчиків, було представлено в [8]. Він базується на поєднанні модифікованих блоків Бруйна та регістра зсуву нелінійних зворотних зв'язків. Два запропоновані екземпляри підходять для захисту недорогих смарт-пристроїв. У [9] важлива відмінна атака на все сімейство ГПВЧ потокових шифрів показує, що майже кожен член цієї родини вразливий до лінійних атак; це може загрожувати безпеці. ГПВЧ з назвою LAMED був представлений в [10] для додатків RFID-міток. Його конструкція заснована на алгоритмі генетичного програмування і має внутрішній стан 64 біти, з 32-бітовим ключем і 32-бітним початковим вектором.

Модульна алгебра, побітові операції XOR та обертання бітів - основні операції, що використовуються для оновлення внутрішнього стану ГПВЧ.

Було запропоновано дві версії генератора. Перший - це 32-розрядний ГПВЧ, а другий - 16-розрядний ГПВЧ. Для перевірки випадковості генераторів використовувались набори статистичних випробувань NIST, ENT та Diehard. Аналіз апаратної складності обох версій генератора підтверджує, що він відповідає вимогам, встановленим недорогою технологією [11], [12]. У [13] було запропоновано J3Gen ГПВЧ на основі попередньої роботи в [14]. J3Gen поєднує в собі TRNG із тепловим шумом та регістр зсуву динамічного лінійного зворотного зв'язку (DLFSR) з n комірок і має чотири основних блоки: СГВЧ на основі генератора, архітектуру DLFSR, логіку декодування та селектор поліномів.

Приблизна апаратна складність цього ГПВЧ підходить для обмежених пристроїв. Розмір ключа захисту відповідає 372 бітам. ГПВЧ J3Gen був успішно підданий криптоаналізу Peinado [15, 16], який показав уразливість алгоритму за допомогою імовірнісної атаки та детермінованої атаки.

Перша дозволяє відновити набір поліномів зворотного зв'язку, які становлять секретну інформацію ГПВЧ. Остання дозволяє зловмисникові відновити всю вихідну послідовність ГПВЧ, знаючи лише кілька бітів послідовності.

Мета – в роботі запропоновано фізичну модель IoT генератора, яка на своєму прикладі надає широкий огляд факторів та обмежень, що виникають під час проектування генераторів. Процес тестування та оптимізації генератора з використанням тестів багатовимірних статистик ілюструє придатність пакету програм до використання і його інтегральну роль в створенні якісного генератора випадкових чисел, в особливості для використання в IoT пристроях.

В роботі розглянуто критерії для перевірки на випадковість бітових послідовностей невеликої довжини (до 100 біт). Даний підхід доцільно використовувати

для тестування полегшеного генератора псевдовипадкових чисел в пристроях з певними обмеженнями на ресурси.

Основна частина дослідження

Властивості генератора псевдовипадкових чисел. Перерахуємо деякі властивості, які повинен мати генератор [17]. Звичайно, потрібно, щоб він виробляв послідовність з рівномірним розподілом на (0, 1).

Це саме по собі є досить абстрактною математичною вимогою; перші дві властивості, наведені нижче, роблять це більш практичним.

1. Пройдіть емпіричні статистичні тести Це тести, де генерується довга послідовність випадкових чисел, а потім потрібно пройти різні статистичні тести, щоб перевірити гіпотезу про те, що числа рівномірно розподілені на [0, 1] і є незалежними.

2. Математична основа За генераторами випадкових чисел (принаймні деякими з них) стоїть багато математичної теорії, включаючи властивості, які повинні створити хороший генератор випадкових чисел.

3. Швидкість (при обмеженій пам'яті) Більшість моделювань вимагають величезної кількості випадкових чисел. Можливо, доведеться сформувати велику кількість вибірок, і генерація кожної вибірки часто передбачає багаторазовий виклик генератора випадкових чисел (ГВЧ). Тож ГВЧ повинен бути швидким.

4. Кілька потоків Легко використовувати паралельні обчислення, але для цього потрібно запустити кілька копій генератора випадкових чисел. Тож потрібно переконатися, що всі ці різні потоки не залежать один від одного.

5. Практичні проблеми Простота установки та легкість генерування. Деякі генератори випадкових чисел досить короткі і займають лише кілька рядків коду. Інші значно складніші. Потрібно переконатися, що отримуються послідовності належним чином.

6. Відтворюваність Для налагодження та тестування потрібно мати можливість генерувати однаковий потік випадкових чисел неодноразово.

Парадокс випадковості

Багатьом захищеним системам необхідно часто генерувати випадкові числа, що суперечить бажанням зменшити кількість подій, які можуть виявити вимірні дані побічного каналу. Щоб створити безпечні секретні ключі, система також повинна використовувати різні початкові числа випадкових чисел кожен раз, коли вона генерує ключ. Таким чином, випливає питання як можна узгодити вимоги до частої генерації випадкових чисел з необхідністю мінімізувати активність для захисту системи від аналізу даних побічного каналу. Одна з проблем, пов'язаних з виконанням цього в цифрових комп'ютерах, полягає в тому, що вони спроектовані так, щоб бути детермінованими, працювати з двійковими даними, щоб усунути невизначеності при маніпулюванні аналоговими сигналами. Створення справжньої випадковості в таких схемах є надзвичайно складною задачею.

Багато різних підходів, які можна для цього використати мають низку недоліків. Які в свою чергу обмежують їх застосовність. Багато ранніх ГВЧ покладалися на час дня, математично комбінуючи цифри, що представляють секунди, десяті, соті і навіть тисячні секунди, для отримання явно випадкового початкового числа.

Однак це початкове число насправді можна розглядати тільки як псевдовипадкове число, тому що результат генерується за допомогою детермінованого процесу, який, якщо його вводити в один і той же час дня, поверне ту ж послідовність «випадкових» чисел. Підхід не проходить перевірку на незалежність, тому що результат передбачуваний. Зловмисник, який може вгадати або, що ще гірше, встановити годинник часу, має можливість значно обмежити кількість можливих початкових значень, використовуваних ГПСЧ, і, отже, може використовувати цю слабкість, щоб порушити безпеку системи. Багато невеликих вбудованих систем, що представляють пристрої IoT, не мають навіть постійних годинників, зберігають своє значення під час перезавантаження або циклів включення живлення. Часто зустрічаються такі системи, які використовують такі функції, як лічильники циклів, для заповнення своїх генераторів випадкових чисел, що призводить до того, що багато копії одного і того ж пристрою генерують одну і ту ж послідовність випадкових чисел з моменту їх скидання. Ці системи просто чекають, щоб їх використовували.

Дизайн генератора випадкових чисел

Одне з основних питань, які потрібно вирішити перед проектуванням та розробкою генератора випадкових чисел, а саме апаратного генератора випадкових чисел (АГВЧ) є вибір датчиків та сенсорів, що будуть використовуватися для генерації випадкових чисел використовуючи фактори навколишнього середовища.

В залежності від обраних факторів навколишнього середовища та варіантів використання генератора необхідно визначитися з датчиками, які будуть збирати інформацію з навколишнього середовища, адже датчик світла не буде корисним, якщо пристрій використовується в темному приміщенні, а датчик руху або акселерометр буде надлишковим для стаціонарного пристрою. Для створюваної моделі генератора це питання треба врахувати, але воно не є настільки критичним як при розробці реального девайсу.

Важливими характеристиками при розробці пристроїв для Інтернету речей є такі як: вага, розміри, об’єм пам’яті, інтеграція з програмним забезпеченням та іншими пристроями тощо.

Мета даної роботи показати підхід до створення легковагового генератора, а також процес тестування, налагодження та оптимізації створеного генератора з використанням програмного засобу для тестування послідовності малої довжини на випадковість з використанням багатовимірних статистик [18], тому, не зважаючи на серйозність цих факторів при розробці пристроїв для кінцевого користувача, ними можна частково знехтувати.

На дизайн генератора більше за все вплинула постановка задачі. Так, типом генератора для моделі було обрано АГВЧ, завдяки тому, що його характеристики дозволять генерувати більш випадкові послідовності. Це рішення в свою чергу викликає необхідність створення фізичної моделі що буде складатися з мікросхеми та декількох сенсорів.

Реальну модель генератора можна побачити на рис. 1.

За основу генератора та мікросхеми було вирішено використати плату Arduino та для моделі було обрано датчик звуку та акселерометр [17].

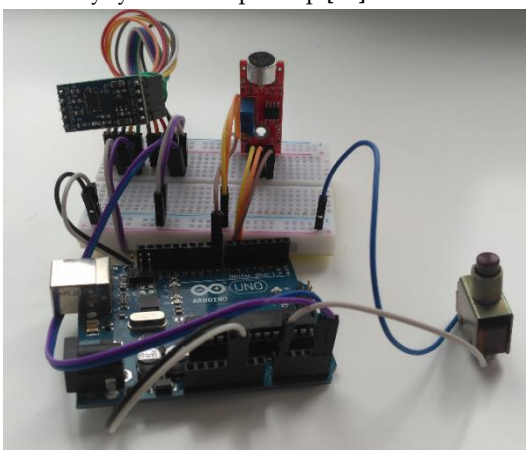


Рис. 1. Фізична модель елементів генератора

На реальній моделі можна побачити сенсори під'єднані до макетної дошки, саму плату Arudino та кнопку. На схемі наявні такі компоненти:

- Датчик звуку;
- Акселерометр;
- Кнопка – тригер;
- Arduino – головна схема генератора.

Варто додати, що генератор створює послідовності довжини 31 біт (короткі послідовності). Пам'ять Arduino є доволі обмеженою, що не дозволить генерувати дуже великі послідовності, але це і не є потрібним, адже в експерименті розглядається саме генерація невеликих послідовностей в контексті легковагових генераторів випадкових чисел.

Методи тестування з використанням багатовимірних статистик

В даному розділі приведемо набори тестів, які будемо використовувати для дослідження згенерованих послідовностей та оптимізації моделі легковагового генератора. Тести багатовимірних статистик відрізняються тільки шаблонами, на які перевіряється послідовність [18-21]. Кожен метод отримує на вхід випадкову величину:

$$\gamma_1, \gamma_2 \ldots, \gamma_n, \quad \text{де } \gamma_i \in \{0, 1\},\ i = 1,2\ldots,n,\ n > 0. \tag{1}$$

Для даної величини визначається кількість специфічних шаблонів k_1, k_2 та k_3 (якщо це визначено методом) і виконується обчислення за допомогою формули специфічної для методу. Перший тест виконується, щоб знайти спільну вірогідність появи подій $k_1 = \eta(tt^*)$ та $k_2 = \eta(t1t^*) + \eta(t0t^*)$, при $t \in \{0, 1\}$, $t^*=1 - t$:

$$\mathrm{P}\left\{\eta\left(tt^*\right) = k_1, \eta\left(t1t^*\right) + \eta\left(t0t^*\right) = k_2\right\} = \sum_{m_1=k_1}^{n-k_1} p^{m_1} q^{m_0} \sum \prod_{i=0}^{1} C_{k_1}^{\delta_i} C_{m_i-k_1}^{k_1-\delta_i}, \tag{2}$$

де n – довжина бітової послідовності, p – вірогідність появи t, q – вірогідність появи t^* ($q = 1 - p$), $m_0 = n - m_1$, $\sum$ - сума по всім комбінаціям δ_0 та δ_1, таким, що: $\delta_0 + \delta_1 = 2k_1 + k_2$.

Другий метод тестування знаходить спільну вірогідність появи подій $k_1 = \eta(tt^*)$ та $k_2 = \eta(ttt^*)$:

$$\mathrm{P}\left\{\eta\left(tt^*\right) = k_1, \eta\left(ttt^*\right) = k_2\right\} = \sum_{m_1=k_1}^{n-k_1} p^{m_1} q^{m_0} C_{k_1}^{k_2} C_{m_1-k_1}^{k_2} C_{m_0}^{k_1}. \tag{3}$$

Третій метод оцінює вірогідність появи шаблонів $k_1 = \eta(tt^*)$, $k_2 = \eta(t1t^*)$ *та* $k_3 = \eta(t0t^*)$:

$$\mathrm{P}\left\{\eta\left(tt^*\right) = k_1, \eta\left(t1t^*\right) = k_2, \eta\left(t0t^*\right) = k_3\right\} = \sum_{m_1=k_1}^{n-k_1} p^{m_1} q^{m_0} C_{k_1}^{k_2} C_{k_1}^{k_3} C_{m_1-k_1}^{k_2} C_{m_0-k_1}^{k_3}. \tag{4}$$

За допомогою четвертого методу можна визначити вірогідність подій $k_1 = \eta(tt^*)$ та $k_2 = \eta(t1t)+ \eta(t0t)$.

$$\mathrm{P}\left\{\eta\left(tt^*\right) = k_1, \eta\left(t1t\right) + \eta\left(t0t\right) = k_2\right\} = \sum_{m_1=k_1}^{n-k_1} p^{m_1} q^{m_0} \times \sum \sum_{i \in \{k_1, k_1+1\}} C_{i-1}^{\delta_0} C_i^{\delta_1 - m_1 + 2i} C_{m_0-i+1}^{k_1-\delta_0} Z\left(m_1 - i, m_1 - i - \delta_1\right),$$

де $\sum$ - сума по всім комбінаціям δ_0 та δ_1, таким, що:

$$\delta_0 + \delta_1 = k_2,\ Z(a,b) = \begin{Bmatrix} C_{a-1}^{b-1}, \text{ якщо } a \ge b \ge 0; \\ 1, \text{ якщо } a = b = 0; \\ 0, \text{ в іншому випадку} \end{Bmatrix}.$$

За допомогою п'ятого методу можна визначити вірогідність подій $k_1 = \eta(tt^*)$ та $k_2 = \eta(ttt)$:

$$\mathrm{P}\left\{\eta\left(tt^*\right) = k_1, \eta\left(ttt\right) = k_2\right\} = \sum_{m_1=k_1}^{n-k_1} p^{m_1} q^{m_0} C_{m_0}^{k_1} \times \sum_{i \in \{k_1, k_1+1\}} C_i^{m_1-k_2-i} Z\left(m_1 - i, m_1 - i - k_2\right). \tag{5}$$

Шостий метод можна використати для того щоб знайти спільну вірогідність подій $k_1 = \eta(tt^*)$ та $k_2 = \eta(tt^*t)$:

$$\mathrm{P}\left\{\eta(tt^*)=k_1,\eta(tt^*t)=k_2\right\}=$$

$$\sum_{m_1=k_1}^{n-k_1} p^{m_1}q^{m_0}\sum_{i\in\{k_1,k_1+1\}} C_i^{k_2}C_{m_0-i}^{k_1-k_2}Z\left(m_1,i+1\right). \quad (8)$$

Сьомий метод шукає спільну вірогідність подій $k_1 = \eta(tt^*)$, $k_2 = \eta(ttt)$ та $k_3 = \eta(tt^*t)$:

$$\mathrm{P}\left\{\eta(tt^*)=k_1,\eta(ttt)=k_2,\eta(tt^*t)=k_3\right\}=\sum_{m_1=k_1}^{n-k_1} p^{m_1}q^{m_0}\times$$

$$\times\sum_{i\in\{k_1,k_1+1\}} C_i^{k_2-m_1+2i}C_{i-1}^{k_3}C_{m_0-i+1}^{k_1-k_3}Z\left(m_1-i,m_1-i-k_2\right). \quad (9)$$

Восьмий метод виконується, щоб знайти спільну вірогідність подій $k_1 = \eta(tt)$ та $k_2 = \eta(t^*t\,t^*)$:

$$\mathbf{P}\left\{\eta(tt)=k_1,\eta(t^*tt^*)=k_2\right\}=\sum_{m_1=0}^{n} p^{m_1}q^{m_0}\times$$

$$\left\{C_{a-2}^{k_2}C_{k_1+1}^{a-k_2+1}Z\left(m_0,a-1\right)+C_a^{k_2}C_{m_0-1}^{a}Z\left(k_1,a-k_2\right)+\right.$$

$$\left.+2C_{a-1}^{k_2}C_{k_1}^{a-k_2-1}C_{m_0-1}^{a-1}+\chi\left(a-1=k_2=m_0=0\right)\right\},$$

де $\chi(E)$ – індикатор події E, $a = m_1 - k_1$.

Тестування, оптимізація та інтерпретація результатів

Тестування згенерованих послідовностей бітів на випадковість буде виконуватися за допомогою методів багатовимірних статистик. Випробування NIST не дадуть якісної оцінки результатів, адже більшість з них розраховані на послідовності, довжина яких більша за 100.

Загальний процес тестування, що буде використано при оцінці генераторів побудовано наступним чином:

– запустити програму за допомогою Arduino та згенерувати деяку кількість випадкових послідовностей;

– виконати тестування послідовностей з використанням восьми методів багатовимірних статистик та реалізованих в пакеті програм;

– знайти відношення між результатами отриманими на попередньому етапі та максимальними значеннями для тесту і відповідної довжини послідовності. Це значення можна знайти за допомогою визначення найбільш вірогідної кількості входжень шаблонів в послідовність;

– зробити висновки про вірогідність послідовності.

Перед тим як розпочати тестування, розглянемо табл. 1, в якій наведено максимальна вірогідність для кожного з тестів багатовимірних статистик. Щоб оцінити наскільки та чи інша послідовність є випадковою, необхідно знайти відношення результатів відповідного тесту до максимальної вірогідності цього тесту. Якщо відношення є більшим за 0,8 то послідовність можна вважати випадковою, якщо ні – вона не є випадковою. Результати тестування 10 послідовностей бітів створених псевдовипадковим генератором на Arduino наведено в табл. 2.

Таблиця 1

Максимальні вірогідності для тестів багатовимірних статистик та довжини послідовності 31

№ Тесту	Найбільша вірогідність
1	0,0699318274855613
2	0,0847552437335252
3	0,0277345534414052
4	0,0368665847927331
5	0,0499579892493784
6	0,0855854991823434
7	0,0172293558716774
8	0,0369482999667525

Таблиця 2

Результати тестування ГПЧ

№ Тесту	1	2	3	4	5	6	7	8
Частина послідовностей що пройшли тест	30%	30%	10%	20%	30%	0%	0%	20%

Результати тестування явно вказують на те, що такі послідовності мають низький рівень випадковості. Оцінити дані можна більш точно, якщо розглянути як показує себе АГВЧ створений з використанням сенсорів (табл. 3). Результати є істотно кращими за ГПЧ і мають загальний позитивний тренд в контексті випадковості. Результати тестування АГВЧ хоч і є позитивними, вказують на те, що цей генератор не створює послідовності належної якості і що його можна потенційно покращити. Однією з проблем зчитування даних з датчиків є те, що дані не змінюються різко і можуть мати загальний тренд.

Таблиця 3

Результати тестування АГВЧ

№ Тесту	1	2	3	4	5	6	7	8
Частина послідовностей що пройшли тест	30%	50%	30%	30%	30%	20%	10%	20%

Цю проблему можна вирішити за допомогою внесення додаткової випадковості в процес генерації послідовності, або винесення детермінованості за межі алгоритму. Одним з підходів, що може бути використано, є Fisher-Yates shuffle [9] – алгоритм, що можна використати для змішування результатів отриманих з датчиків. Результати явно вказують на те, що змішування даних отриманих з сенсорів мало позитивний вплив на випадковість послідовностей створюваних генератором. Наостанок, розглянемо послідовності згенеровані під час

того, як генератор та сенсори знаходилися в відносному спокої (табл. 5).

Таблиця 4

Результати тестування АГВЧ, що використовує алгоритм Fisher-Yates shuffle

№ Тесту	1	2	3	4	5	6	7	8
Частина послідовностей що пройшли тест	60%	50%	30%	50%	50%	40%	30%	40%

Таблиця 5

Результати тестування АГВЧ в стані відносного спокою

№ Тесту	1	2	3	4	5	6	7	8
Частина послідовностей що пройшли тест	20%	20%	10%	10%	10%	20%	10%	10%

Як можна побачити з результатів, коли сенсори не отримують постійних випадкових даних, в послідовностях що створює генератор з'являється висока детермінованість. Відповідно, даний генератор потребує поліпшення на випадок ситуації відносного спокою.

Практичні рекомендації

Перед тим як застосовувати ланцюжки випадкових чисел для моделювання реальної практичної задачі бажано дотримуватися наступних порад:

– Не використовувати вбудований ГПВ, якщо невідомо як він сконструйований, алгоритм його роботи і як він був протестований.

– Потрібно сконструювати свій код таким чином, щоб було легко змінити його в створеному легковаговому генераторі псевдовипадкових чисел, який ви використовуєте.

– Бажано використовувати два різні ГПВЧ і порівнювати їх результати. Це не втрата часу, оскільки завжди можна поєднати два набори даних. Бажано сконструювати другий генератор таким чином, щоб він використовував відмінні від першого генератора фактори навколишнього середовища та інші датчики для збору цих факторів. Або якщо не планується розробка ще одного генератора, то можна скористатися підходом при якому використовується лише кожне п'яте значення випадкового числа з генератора.

– Доцільно не використовувати занадто багато випадкових чисел з генератора порівняно з його періодом.

Висновки

Аналіз галузі розробки та побудови легковагових генераторів дозволив обґрунтувати необхідність побудови пакетів тестів для перевірки на випадковість послідовностей, які є результатом генерації пристроїв з певними обмеженнями.

Виконаний аналіз вказує на те, що існуючі тести мають низку недоліків, вирішення яких може зменшити передумови до тестування та покращити точність отриманих результатів. Робота присвячена доволі актуальній задачі – дослідженню генераторів випадкових чисел, які працюють на пристроях з обмеженими ресурсами, та послідовностей невеликої довжини на випадковість.

В роботі було розглянуто побудову фізичної моделі легковагового генератора псевдовипадкових чисел. Використання багатовимірних статистик як основи для випробувань, дозволяє краще дослідити послідовність на випадковість, за рахунок оцінки одночасно декількох характеристик послідовності. Тести багатовимірних статистик засновані на дослідженні входжень шаблонів в послідовність і допомагають виявляти приховані залежності між даними та неякісні генератори. Головною перевагою цих тестів є їх ефективність на послідовностях короткої довжини, тому вони вирішують одну з проблем існуючих тестів, полегшуючи передумови до випробувань.

Фізична модель IoT генератора представлена в роботі, на своєму прикладі надає широкий огляд факторів та обмежень, що виникають під час проектування генераторів.

Процес тестування та оптимізації генератора з використанням тестів багатовимірних статистик ілюструє придатність пакету програм до використання і його інтегральну роль в створенні якісного генератора випадкових чисел, в особливості для використання в IoT пристроях. Програмний продукт, що було створено в цій роботі може використовуватися для вирішення широкого спектру задач.

Література

[1] Chugunkov I. V., Novikova O. Y., Perevozchikov V. A. and Troitskiy S. S., "The development and researching of lightweight pseudorandom number generators," *2016 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW)*, 2016. - pp. 185-189.

[2] Ullah I., Meratnia N. and Havinga P. J. M., "Entropy as a Service: A Lightweight Random Number Generator for Decentralized IoT Applications," *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2020. - pp. 1-6.

[3] Dinca L. M., Hancke G., "Behavioural sensor data as randomness source for iot devices", *2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), June 2017*, 2017. - pp. 2038-2043.

[4] Francis L., Hancke G., Mayes K. and Markantonakis K., "Potential misuse of nfc enabled mobile phones with embedded security elements as contactless attack platforms", *2009 International Conference for Internet Technology and Secured Transactions (ICITST)*, Nov 2009, 2009. - pp. 1-8.

[5] Orue A., Hernandez L., Montoya F., "Trifork, a new Pseudorandom Number Generator Based on Lagged Fibonacci Maps". *Journal of Computer Science and Engineering*, 2(2), 2010. – pp. 46-51.

[6] Francillon A., Castelluccia C., "Tinyrng: A cryptographic random number generator for wireless sensors network nodes". *IEEE 2007 5th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, 2007. - pp.1–7.

[7] Lo Re G., Milazzo E., Ortolani M., Secure random number generation in wireless sensor networks. ACM *Proceedings of the 4th International Conference on Security of Information and Networks (SIN'11)*, 2011. - pp.175– 182.

[8] Gaglio V., Paola A., Ortolani M., Lo Re G., "A TRNG exploiting multi-source physical data." *ACM Proceedings of the 6th Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet'10)*, 2010. - pp.82–89.

[9] Mandal K., X. Fan, and G. Gong, Design and implementation of Warbler family of lightweight pseudorandom number generators for smart devices. *ACM Transactions on Embedded Computing Systems*, 2016. – pp. 1-28.

[10] Mabin J., G. Sekar, and R. Balasubramanian, Distinguishing Attacks on (Ultra-)Lightweight WG Ciphers. *5th International Workshop Lightweight Cryptography for Security and Privacy (LightSec 2016)*, LNCS 10058, 2017. - pp.45–59.

[11] Peris-Lopez P., Hernandez-Castro J. C., Estevez-Tapiador J. M., Ribagorda A. "LAMED – a PRNG for EPC Class-1 Generation-2 RFID specification". *Computer Standards and Interfaces*, 31(1), 2009. –pp. 88-97.

[12] Markku - Juhani O., Saarinen, D.E. "A Do-It-All-Cipher for RFID: Design Requirements (Extended Abstract)". *Cryptology ePrint Archive, Report* 2012/317, 2012. – 54 p.

[13] Martın H., Peris-Lopez P., Tapiador J.E., San Millan E. "An estimator for the ASIC footprint area of lightweight cryptographic algorithms" *IEEE Transactions on Industrial Informatics* 10(2), 2014. – pp.1216–1225.

[14] Melia-Segu J., Garcia-Alfaro J., Herrera-Joancomartı J. "J3Gen: *A PRNG for low-cost passive RFID" Sensors*, 2013. - pp. 3816–3830.

[15] Melia-Segu J., J. Garcia-Alfaro, J. Herrera-Joancomartı, "Multiplepolynomial LFSR based pseudorandom number generator for EPC Gen2 RFID tags". *37th Annual Conference of the IEEE Industrial Electronics Society (IECON 2011)*, 2011. - pp. 3820–3825.

[16] Peinado A., Munilla J., Fuster-Sabater A. "EPCGen2 Pseudorandom Number Generators: Analysis of J3Gen". *Sensors*. - 14(4), 2014. – pp. 6500-6515.

[17] Райчев О.О. Засіб тестування IoT генераторів випадкових чисел з використанням багатовимірних статистик: бакалаврська робота. Київський національний університет імені Тараса Шевченка, Київ, 2021.

[18] Поперешняк С.В. Програмний засіб для тестування бітової послідовності малої довжини на випадковість // *Безпека інформації*. – т. 27 (2), 2020. – С. 80-86.

[19] Popereshnyak S., Dimitrov G. The Testing of Pseudorandom Sequences using Multidimensional Statistics *Proceedings of the 1st International Workshop on Digital Content & Smart Multimedia (DCSMart 2019)* Lviv, Ukraine, December 23-25, 2019. - pp. 151-161.

[20] Masol V., Popereshnyak S. Statistical analysis of local sections of bits sequences // *Journal of Automation and Information Sciences*. Vol. 51, 2019. - pp. 31-45.

[21] Masol V., Popereshnyak S. Checking the Randomness of Bits Disposition in Local Segments of the (0, 1)-Sequence //*Cybernetics and Systems Analysis* 56(3). 2020. - pp. 1-8.

УДК 519.212.2 : 681.51

Поперешняк С.В., Райчев А.О. Исследования и тестирование легковесных генераторов псевдослучайных чисел для интернета вещей

Аннотация. *Анализ случайных последовательностей и генераторов случайных чисел является довольно специфической задачей, но для ее решения может быть использован один или несколько из многочисленных пакетов тестов. Однако, выполненный анализ указывает на то, что существующие методы тестирования имеют ряд недостатков, решение которых может уменьшить предпосылки к тестированию и улучшить точность полученных результатов. Работа посвящена довольно актуальной задачи - исследованию генераторов случайных чисел, работающих на устройствах с ограниченными ресурсами, и последовательностей небольшой длины на случайность. В работе было рассмотрено построение физической модели легковесного генератора псевдослучайных чисел. Использование многомерных статистик в качестве основы для испытаний, позволяет лучше исследовать последовательность на случайность, за счет оценки одновременно нескольких характеристик последовательности. Тесты многомерных статистик, которые основанные на исследовании*

вхождений нескольких шаблонов в последовательность, помогают выявлять скрытые зависимости между данными и некачественные генераторы. Главным преимуществом этих тестов является их эффективность на последовательностях короткой длины, поэтому они решают одну из проблем существующих тестов, облегчая предпосылки к испытаниям. Представленная в работе физическая модель IoT генератора на своем примере предоставляет широкий обзор факторов и ограничений, которые возникают при проектировании генераторов. Процесс тестирования и оптимизации генератора с использованием тестов многомерных статистик иллюстрирует пригодность пакета программ к использованию и его интегральную роль в создании качественного генератора случайных чисел, в особенности для использования в IoT устройствах. Программный продукт, что был создан в этой работе может использоваться для решения широкого спектра задач, как уже и было неоднократно отмечено. Одной из важнейших, и действительно той, что может получить неоценимую пользу сферой применения является криптография.
Ключевые слова: *легковесный генератор псевдослучайных чисел, тестирование, многомерная статистика, интернет вещей, криптография.*

Popereshnyak S. V., Raichev O.O. The research and testing of lightweight pseudorandom number generators for the Internet of Things

Abstract. *The analysis of random sequences and random number generators is a rather specific task, but one or more of the numerous test packages can be used to solve it. However, the analysis performed indicates that the existing testing methods have a number of disadvantages, the solution of which can reduce the prerequisites for testing and improve the accuracy of the results. The work is devoted to a rather urgent problem - the study of random number generators operating on devices with limited resources, and short-length sequences for randomness. The paper considered the construction of a physical model of a lightweight pseudo-random number generator. By using multivariate statistics as a basis for testing, it is possible to better investigate a sequence for randomness by evaluating several characteristics of the sequence simultaneously. Tests of multivariate statistics, which are based on the study of occurrences of several patterns in a sequence, help to reveal hidden dependencies between data and low-quality generators. The main advantage of these tests is their effectiveness on short sequences, so they solve one of the problems of existing tests, facilitating the prerequisites for testing. The physical model of the IoT generator presented in the work, by its example, provides a broad overview of the factors and limitations that arise in the design of generators. The process of testing and optimizing the generator using tests of multivariate statistics illustrates the suitability of the software package for use and its integral role in creating a quality random number generator, especially for use in IoT devices. The software product that was created in this work can be used to solve a wide range of tasks, as has already been repeatedly noted. One of the most important, and indeed the one that can receive invaluable benefits in the field of application, is cryptography.*
Keywords: *lightweight pseudorandom number generator, testing, multivariate statistics, internet of things, cryptography.*

Поперешняк Світлана Володимирівна, к.ф.-м.н., доцент, доцент кафедри програмних систем і технологій Київського національного університету імені Тараса Шевченка.
Поперешняк Светлана Владимировна, к.ф.-м.н., доцент, доцент кафедры программных систем и технологий Киевского национального университета имени Тараса Шевченко.
Popereshnyak Svitlana, Ph.D., assistant Professor of the Department of Software Systems and Technologies, Taras Shevchenko National University of Kyiv.

Райчев Олексій Олегович, магістр кафедри програмних систем і технологій Київського національного університету імені Тараса Шевченка.
Райчев Алексей Олегович, магистр кафедры программных систем и технологий Киевского национального университета имени Тараса Шевченко.
Raichev Oleksiy, Master of the Department of Software Systems and Technologies, Taras Shevchenko National University of Kyiv.

Отримано 20 *червня 2021 року,* затверджено редколегією *27 серпня 2021 року*

ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

ОРГАНІЗАЦІЙНО-ПРАВОВІ ПИТАННЯ БЕЗПЕКИ ІНФОРМАЦІЇ / ORGANIZATIONAL AND LEGAL ISSUES OF INFORMATION SECURITY

DOI: 10.18372/2225-5036.27.16004

СТАНОВЛЕННЯ УКРАЇНСЬКОЇ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ. 1991–1994.

Валерій Ворожко

Національний авіаційний університет, Галузевий державний архів СБ України

ВОРОЖКО Валерій Павлович, к.іст.н.
Рік та місце народження: 1953 рік, м. Гагра, Грузія.
Освіта: Московський державний історико-архівний інститут, 1975 рік.
Посади: доцент кафедри безпеки інформаційних технологій НАУ, провідний науковий співробітник Галузевого державного архіву СБ України.
Наукові інтереси: історія спецслужб та військової промисловості.
Публікації: більше 60 наукових публікацій, серед яких монографії, навчальні посібники, наукові статті.
E-mail: wp06vv@gmail.com.
Orcid ID: 0000-0003-1262-1376.

Анотація. *У статті на підставі законодавчих актів України, праць українських дослідників та архівних документів ЦДАВО України розглядаються процеси формування державних органів України, відповідальних за інформаційну безпеку, створення системи охорони державної таємниці, урядового зв'язку, технічного захисту інформації з обмеженим доступом у 1991–1994 рр. Привернута окрема увага до нормативно-правових актів України щодо захисту державної таємниці та до діяльності Державного комітету України з питань державних секретів. Автором проаналізовані: стан справ з таємницями військової промисловості та військового відомства, що залишилися у спадок від колишнього СРСР, а також Угода пострадянських країн про взаємне забезпечення збереження міждержавних секретів. Систематизовані носії таємної інформації, що перебували на той час в обігу або на зберіганні в режимно-секретних органах. Зроблено порівняння радянської та української систем охорони державної таємниці. Досліджено процес формування першого українського Зводу відомостей, що містять державну таємницю. Проведено порівняльний аналіз функцій Держкомсекретів України та Служби безпеки України з функціями державних органів США, відповідальних за охорону державних таємниць, таких як Управління з нагляду за інформаційною безпекою (ISOO) та Федерального бюро розслідувань (FBI). Розглянуті функції українського інституту «державних експертів з питань таємниць» та проблемні питання матеріального стимулювання діяльності громадян за роботу в умовах режимних обмежень. Наведені приклади реліктових залишків радянської цензури та розглянуто процес трансформації цензорських органів України. Методологія дослідження спирається на принципи об'єктивності, позитивізму, системності, історизму та базується на історичних методах: проблемно-хронологічному, історико-порівняльному, історико-правовому.*

Ключові слова: *Держкомсекретів, СБ України, СОДТ, таємні відомості, таємні документи, технічний захист інформації, урядовий зв'язок.*

Вступ

Метою цієї роботи є необхідність підвищення ефективності вітчизняної системи охорони державної таємниці та технічного захисту інформації на основі історичного досвіду становлення української системи охорони державної таємниці.

Актуальність праці обумовлюється нинішнім протистоянням України потужним зусиллям своїх зовнішніх і внутрішніх ворогів, мета яких – ліквідація української державності, знищення української нації та України як суб'єкта міжнародного права і геополітичної реальності.

Сучасні суспільно-політичні виклики зумовлюють необхідність об'єктивного аналізу всіх складових 30-річного функціонування «державного організму» України та його трансформації в сучасну демократичну країну.

24 серпня 1991 р. Верховна Рада (далі – ВР) УРСР проголосила незалежність України та прийняла основоположні рішення, спрямовані на створення власної держави. Проголошення курсу на розбудову демократичної держави зумовило потребу створення національної системи охорони державної таємниці (далі – СОДТ), яку передбачалося створити з урахуванням змін в економіці, політичній та соціальній сферах, розвитку міжнародного співробітництва та світової практики створення подібних систем.

Важливим завданням для України на той період було подолання негативних наслідків минулого політичного режиму, а саме тотальної засекреченості в усіх сферах діяльності держави та суспільства.

Аналіз джерел і публікацій

Історіографія досліджень побудови Україною національної системи охорони державної таємниці нараховує низку публікацій. Окремі питання вже висвітлювалися у працях автора цієї публікації, як одноосібних [1–4], так і в співавторстві [5–6].

Автором використані документи Центрального державного архіву вищих органів влади і управління України (далі – ЦДАВО України) та Галузевого державного архіву СБ України (далі – ГДА СБУ).

Основна частина дослідження

Радянська СОДТ формувалася в умовах військово-мобілізаційної моделі розвитку економіки, тотального політичного контролю та була ієрархічною адміністративною структурою, яка віддзеркалювала характер взаємин суспільства й тоталітарної держави. Витоки надзвичайно складної ситуації в сучасній Україні, що спричинені зовнішньою агресією та сепаратистськими проявами, значною мірою криються саме у спадщині радянського тоталітарного режиму, якому була притаманна серед іншого, надзвичайна закритість. Нормативно-правове забезпечення СОДТ у СРСР здійснювалося на підставі низки розрізнених підзаконних нормативно-правових актів державних органів, а не відповідно до єдиного узагальнюючого законодавчого акту. Головними серед них були інструкції з питань режиму секретності, які затверджувались вищим виконавчим органом влади.

У країні було створено нормативно-правову базу, що забезпечувала функціонування адміністративно-правових режимів, які в сукупності та взаємодії забезпечували збереження державної таємниці.

На початковому етапі для охорони державної таємниці в незалежній Україні продовжувала застосовуватися система радянського періоду. Серед перших правових актів, прийнятих у державі, була постанова ВР України від 12 вересня 1991 р. «Про порядок тимчасової дії на території України окремих актів законодавства Союзу РСР», яка визначала, що до прийняття відповідних актів законодавства України на території республіки застосовуються акти законодавства СРСР з питань, які не врегульовані законодавством України, за умови, що вони не суперечать Конституції і законам України [7]. У сфері охорони державної таємниці головним нормативним документом залишалася «Інструкція із забезпечення режиму секретності в міністерствах, відомствах, на підприємствах, установах і організаціях СРСР» № 556-126 від 12 травня 1987 р. [8, арк. 283–456].

Поряд з іншими завданнями, що постали перед Україною, не останнє місце займало створення власних органів державної безпеки (контррозвідки), побудова яких проходила з урахуванням досвіду організаційно-правового забезпечення, наявного кадрового потенціалу, матеріально-технічної бази КДБ УРСР. 20 вересня 1991 р. парламент України ухвалив постанову «Про створення Служби національної безпеки України» (далі – СНБУ) [7].

На підставі цього акту до обрання Президента України новостворена служба мала підпорядковуватися Голові ВР України. У середовищі співробітників КДБ УРСР не було єдиної позиції щодо переходу на службу у формування національної безпеки нової України.

Велика частина співробітників КДБ УРСР, здебільшого росіян за походженням, категорично не сприймала перспективи прийняття Присяги Україні і шукала шляхи переходу в органи безпеки РФ та готувалась до виїзду з України, ще одна частина співробітників, які хоча і були українцями за походженням, але присвятили своє життя боротьбі в Україні зі всім українським, і тому світоглядно не сприймали перспективи служіння незалежній Україні й також готувались до звільнення зі служби. Ще одна частина співробітників вагалася, яку долю собі обрати [9, с. 240]. Для значної частини співробітників головною мотивацією вибору були матеріальні аспекти. Із 2 січня 1992 р. наказом Голови СНБУ № 01 всі відділи військової контррозвідки по військових, прикордонних округах, внутрішніх військах, флоту, окремих

арміях, корпусах, дивізіях та їм рівних, дислокованих на території України, були підпорядковані Управлінню військової контррозвідки СНБУ [6, с. 130–131]. Постановою ВР України від 18 лютого 1992 р. був введений у дію Закон України «Про оперативно-розшукову діяльність», який визначив, зокрема, таку підставу для проведення оперативно-розшукової діяльності, як запити державних органів, установ та організацій про перевірку осіб на допуск до державної таємниці [7].

Реорганізаційні процеси, пов'язані з колишнім КДБ, були завершені на початку 1992 р. Постановою ВР України від 25 березня вводився в дію Закон України «Про Службу безпеки України», яким було встановлено, що на перейменований орган державної безпеки покладаються, серед інших, завдання оперативного забезпечення, участі у розробці та здійсненні заходів щодо захисту державної таємниці України та досудового слідства про злочини у цій сфері діяльності [7]. З того часу почалось поетапне реформування Служби безпеки України (далі – СБ України), яке триває й донині.

Після ліквідації СРСР у нашій державі відбувався розпад радянської СОДТ, яка поступово вступала в суперечність із законодавством України. Кабінет Міністрів України (далі – КМ України) прийняв 13 квітня 1992 р. протокольне рішення «Про захист таємної та службової інформації», спрямоване на підвищення відповідальності керівників усіх рівнів за забезпечення режиму секретності, розробку та здійснення ефективних заходів для збереження державної таємниці, виключення несанкціонованих випадків передачі за межі України таємних носіїв інформації [1, с. 30]. Прийняте рішення було важливим кроком у сфері охорони таємної інформації, однак воно не вирішувало існуючих проблем. У жовтні 1992 р. Управління урядового зв'язку СБ України, яке забезпечувало лише експлуатацію регіональної частини спеціального зв'язку, було реорганізовано в Головне управління урядового зв'язку, основним завданням якого стало створення урядового зв'язку незалежної держави. Протягом порівняно короткого періоду успадкований фрагмент системи урядового зв'язку поступово був перетворений у цілісну Державну систему урядового зв'язку [10, с. 7–8], яка вважалася умовно ефективною до 2014 р., поки російська агресія не виявила її безпорадність у багатьох аспектах. Витік таємної (конфіденційної) інформації з каналів урядового зв'язку до Кремля відбувався аж до «касетного скандалу» 2001 р. Стратегія радикальних українських реформ, – на думку Ю. Костенка, – яку комуністична більшість ВР України у 1991–1994 рр. спрямувала у річище «поступових кроків» під керівництвом радянських професіоналів, і є причиною того жалюгідного стану, в якому перебуває Україна. Це певною мірою стосується й СБ України, поліції, судової гілки влади, частини збройних сил, економіки, освіти, які й донині залишаються у черговій стадії кволого реформування [11, с. 236].

Основними продуцентами державних секретів у радянські часи були військові формування та військова промисловість (далі – ВП). Особливих проблем із переходом військових таємниць під український прапор не було. Так, 23 грудня 1991 р. наказом Міноборони (далі – МО) України № 03 було створено управління шифрованого зв'язку і режиму секретності Збройних сил України. Станом на 1 січня 1992 р. у військах (силах), які дислокувалися (базувалися) в Україні та перейшли під українську юрисдикцію було 7483 секретних частин і мобілізаційних діловодств. Загалом персонал шифрувальних органів і режимно-секретних органів (далі – РСО) Міноборони складав понад 18 тис. осіб. 5 січня 1992 р. МО України затвердило Положення «Про Управління шифрованого зв'язку і режиму секретності (Восьме управління) МО України» та визначило його статус як центрального шифрувального і режимно-секретного органу Збройних сил України [12, с. 465].

Набагато складнішою склалася ситуація з таємницями ВП, що залишилася у спадок від колишнього СРСР. Усі підприємства й організації ВП, які розташувалися на території УРСР, у радянські часи були підпорядковані 9 міністерствам оборонних галузей промисловості.

Крім так званої «дев'ятки», оборонні замовлення розміщувалися на підприємствах та в наукових установах інших відомств. Точна їхня чисельність, кількість працівників, таємних паперових носіїв і виробів була невідома. На той час наводилися різні дані про наявність в Україні підприємств ВП чисельністю від 700 до 3594.

Найавторитетнішим джерелом можна вважати Наукову доповідь Національного інституту стратегічних досліджень «Національна безпека України, 1994–1996 рр.», в якій зазначено, що «у 1991 р. майже 700 підприємств [України] виробляли продукцію військового призначення» [13, с. 81–82]. На думку автора і ця цифра завищена. Ймовірно до цих підприємств були зараховані й підприємства, які мали лише мобілізаційне замовлення на вироби подвійного призначення і мали РСО у складі 1-ї штатної особи або сумісника.Постановою КМ України від 29 жовтня 1991 р. № 297 був створений Державний комітет України по оборонній промисловості і машинобудуванню. Серед його «питань» забезпечення охорони державної таємниці не згадувалося. 29 квітня 1992 р. Постановою КМ України № 217 комітет ліквідували і на його базі створили Міністерство машинобудування, ВПК і конверсії до якого увійшли установи і підприємства колишніх 16 союзних міністерств, зокрема 9 міністерств оборонних галузей промисловості [14, арк. 89].

Про забезпечення охорони державної таємниці також не згадувалося. Водночас у постанові був зазначений «спеціальний режим» на підприємствах.

Із розпадом СРСР значна частина радянських державних секретів перетворилася у міждержавні. Враховуючи цей аспект, а також величезний обсяг матеріальних носіїв міждержавних секретів та продовження співробітництва, 22 січня 1993 р. у Мінську між урядами країн Співдружності незалежних держав було підписано «Угоду про взаємне забезпечення збереження міждержавних секретів» (далі – Угода).

До Угоди додавалися «Загальні принципи забезпечення режиму секретності при здійсненні політичного, економічного, науково-технічного і військового співробітництва між державами – учасниками Угоди про взаємне забезпечення збереження міждержавних секретів».

Під терміном «міждержавні секрети» розуміли визначені відповідно до внутрішнього законодавства сторін державні секрети, передані цими сторонами в рамках здійснення співробітництва в порядку, встановленому кожною зі сторін, а також секрети, що створювалися в процесі спільних робіт [6, с. 135]. Ця Угода з'явилася за ініціативою й в інтересах РФ, яка використовувала її як «м'яку силу» для контролю процесів розсекречування таємних документів і виробів.

Це, зокрема обмежувало експортні можливості у торгівлі товарами військового призначення на зовнішніх ринках країнами, які підписали Угоду, передусім України і Білорусі. Україна виконувала угоду сумлінно і цим часто користувалася Білорусь, яка ігнорувала Угоду, якщо вона їй була не вигідна.

Таємні носії інформації, які на той час накопичились і перебували в обігу, умовно можна розподілити на декілька груп: а) яким надано гриф секретності «особой важности», «совершенно секретно», «секретно» на підставі відомчих переліків відомств колишнього СРСР до 1991 р. і які мали міждержавний характер; б) яким надано гриф секретності «особой важности», «совершенно секретно», «секретно» на підставі відомчих переліків відомств колишніх СРСР та УРСР до 1991 р. і які не мали міждержавного характеру, тобто автором і власником цієї інформації була Україна; в) яким надано гриф секретності «особливої важливості», «цілком таємно», «таємно» на підставі відомчих переліків відомств колишніх СРСР та УРСР після 24 серпня 1991 р.

Українські грифи обмеження доступу «особливої важливості», «цілком таємно», «таємно» до прийняття власного законодавства щодо державної таємниці були тільки перекладом на українську мову радянських грифів і не несли повноцінного правового навантаження. Офіційна процедура розсекречування розпочалася у 1992 р. спочатку лише щодо архівних документів КПРС з грифами «совершенно секретно» і «особая папка» в системі Головного архівного управління при КМ України на підставі наказу голови Головархіву України від 2 квітня 1992 р. №14 [15, с. 33]. До 2010–2014 рр. процес розсекречування в Україні через радянські стереотипи й агентів впливу РФ всіляко гальмувався.

Щодо цензури в той час також зберігалися радянські стереотипи. На початку 1992 р. постановою КМ України від 3 січня № 6 було створено Головне управління по охороні державних таємниць у пресі та інших засобах масової інформації при КМУ (ГУОТ України) як правонаступник Укрголовліту – цензорського органу УРСР [6, с. 137].

Постановою КМ України від 10 листопаду 1992 р. № 616 на базі ГУОТ був створений Державний комітет України з питань охорони державних таємниць у пресі та інших ЗМІ (далі – Держкомтаємниць України) [6, с. 139].

Першим законодавчим актом, що стверджував інформаційний суверенітет України, став Закон України «Про інформацію», прийнятий ВР України 2 жовтня 1992 р. [7]. Цей Закон визначив режим доступу до інформації, поділивши її на відкриту інформацію та інформацію з обмеженим доступом, закріпив за державою право і обов'язок здійснювати контроль за режимом доступу до інформації.

Указом Президента України від 1 грудня 1992 р. № 593/92 була створена Державна служба України з питань технічного захисту інформації (далі – ДСТЗІ), на яку покладалися функції щодо реалізації державної політики, організаційного, нормативного, інженерно-технічного забезпечення технічного захисту інформації [6, с. 140].

На той час уся діяльність у цій сфері здійснювалася на підставі нормативних документів, затверджених Держтехкомісією СРСР/РФ[1]. ДСТЗІ підписала декілька угод про співробітництво з Держтехкомісією РФ та перебувала у фарватері політики РФ у сфері технічного захисту інформації (далі – ТЗІ).

Одним із питань на підготовчому етапі формування власної СОДТ було визначення державного органу як спеціально уповноваженого органу державної влади з головним завданням реалізації державної політики у цій сфері діяльності.У той період існувала думка, що формування СОДТ, аналогічної радянському режиму, могло б створити передумови для зловживань щодо застосування таємної інформації, порушень прав і свобод людини. Демократизація правовідносин у сфері, пов'язаній з державною таємницею, повинна була передбачати розширення прав і, водночас,

[1] Державний орган СРСР/РФ який відповідав за протидію іноземним технічним розвідкам і ТЗІ.

підвищення відповідальності керівників усіх рівнів за режим секретності та персоніфікацію питань щодо віднесення відомостей до державної таємниці та їхнього засекречування.

Тому було прийнято рішення про створення окремого спеціального уповноваженого органу державної влади з питань охорони державної таємниці відповідно до досвіду США та в цілому євроатлантичної СОДТ. Ця ідея тоді викликала спротив у проросійської частини української верхівки, яка з часом значно посилилася й в 1999 р. українську СОДТ значною мірою повернули до радянсько-російської моделі. Визначений ВР України політичний курс щодо формування СОДТ був реалізований відповідними рішеннями уряду держави. Постановою КМУ від 4 травня 1993 р. № 327 було створено Державний комітет України з питань державних секретів (далі – ДКС України) [7], який функціонально був побудований схожим до Управління з нагляду за інформаційною безпекою **(Information Security Oversight Office, далі – ISOO), у складі NARA (Національне агентство з питань документації і архівів) США.** ISOO відповідає за впровадження та реалізацію президентських виконавчих наказів у сфері таємниць; розробляє стандарти для засекречування і розсекречування документів та типові інструкції з охорони таємних відомостей, займається підвищенням кваліфікації спеціалістів РСО; проводить перевірки в установах на їхню відповідність політиці уряду у галузі інформаційної безпеки; реагує на скарги та пропозиції установ і громадян щодо засекречування та розсекречування інформації; вносить пропозиції Президентові щодо змін у політиці інформаційної безпеки; збирає відповідні звіти з установ, узагальнює їх і готує щорічний звіт з інформаційної безпеки Президенту США тощо [16, с. 26].

ВР України вже на етапі прийняття законів, які регламентували діяльність СБ України, залишила за цим державним органом лише функції спеціальної компетенції як правоохоронного органу. **Функції СБ України у сфері охорони таємниць набули рис схожих до подібних функцій Федерального бюро розслідувань США.**

Постановою КМ України 16 червня 1993 р. № 458 було затверджено положення про ДКС України, яким встановлено, що він є центральним органом державної виконавчої влади, підвідомчим КМ України, який «[...] забезпечує у межах своїх повноважень проведення державної політики з питань захисту державних секретів, реєструє відомості, що становлять державну таємницю, організує, координує і контролює режимно-секретну діяльність державних органів, підприємств, установ і організацій незалежно від форм власності, дипломатичних представництв та інших об'єктів України за кордоном» [7].

У серпні 1993 р. Держкомсекретів України ініціював проведення загальнодержавної наради з проблем охорони державної таємниці [14, арк. 131]. Така нарада відбулася 9 грудня 1993 р. під керівництвом віце-прем'єр-міністра В. Шмарова. У роботі наради взяли участь 217 представників ВР України, Адміністрації Президента України, КМ України, міністерств, відомств, підприємств, установ, що здійснювали діяльність, пов'язану з державною таємницею [14, арк. 2]. У доповіді В. Шмарова, зокрема, зазначалося, що «[…] спостерігається тенденція до розвалу РСО, розширюється діапазон каналів витоку таємної інформації, розбазарюються науково-дослідні, конструкторські розробки, винаходи і пріоритетні технології, що може призвести до непоправних утрат для економіки, оборони й безпеки держави. Значна частина державних секретів та іншої інформації, яка охороняється, перебуває в галузі науково-дослідних і дослідно-конструкторських робіт в інтересах оборони і безпеки держави. Підприємства і організації, що працюють в цій галузі, опинилися у тяжкому становищі.

Низька заробітна плата – одна з головних причин відтоку кваліфікованих наукових кадрів зі структур, що працюють на оборону і безпеку, і передусім молодих перспективних вчених. Багато з них переходить на підприємства і в установи, що діють в умовах вільного ціноутворення, зокрема, в спільні фірми та інші структури, які діють під іноземним контролем.

Це створює передумови до розголошення таємних відомостей, призводить до витоку «умів» і є великою державною проблемою […]» [14, арк. 31]. Він також зазначив, що станом на 1993 р. «[…] в Україні діє близько 20 тис. РСО, зокрема 13 тис. у цивільних відомствах, 7 тис. у військовому відомстві, крім того є близько 4 тис. шифрувальних органів.

Через об'єктивні, а часом і суб'єктивні причини скорочується чисельність працівників РСО. На підприємствах Мінмашпрому скорочено більше половини працівників РСО» [14, арк. 38].

У країні залишилося від радянських замовлень понад 133 млн. таємних документів, декілька сотень тис. таємних виробів, понад дві тисячі виконуваних і незавершених науково-дослідних та дослідно-конструкторських робіт [17, арк. 29–52].

Водночас сумлінне та відповідальне виконання своїх обов'язків працівниками РСО врятувало загальну ситуацію щодо збереження носіїв таємної інформації від катастрофи. У 1993 р. про це перший віце-президент НАН України В. Бар'яхтар висловився так: «[…] слід відзначити, що незважаючи на скрутне економічне становище, в якому ми опинилися, Академія наук України змогла зберегти систему захисту державних секретів у сфері фундаментальних і прикладних досліджень академічної науки. Їхній захист порівняно з умовами колишнього СРСР майже не змінився. Це і не дивно – по-перше, цей захист забезпечується підзаконними актами

колишнього Союзу, а по-друге, – його забезпечує «гвардія начальників перших відділів» – переважно кваліфікованих кадрів» [14, арк. 71].

Постановою ВР України від 21 січня 1994 р. № 3855-12 було введено в дію Закон України «Про державну таємницю» [7]. Правові норми цього Закону передбачали створення СОДТ з урахуванням досвіду розвинених демократичних країн. Звичайно, було використано і радянський досвід охорони державної таємниці. Спеціально уповноваженим центральним органом державної виконавчої влади у сфері забезпечення охорони державної таємниці визначили ДКС України. Було також встановлено, що окремі функції у цій сфері, зокрема щодо ТЗІ, оперативних заходів охорони державної таємниці, фельд'єгерського зв'язку, охорони державної таємниці у засобах масової інформації виконують відповідні державні органи в межах повноважень, передбачених законодавством. Закон, єдиний в СНД, передбачав створення інституту державних експертів з питань таємниць, тільки рішеннями яких інформація могла бути віднесена до державної таємниці. На підставі мотивованих рішень державних експертів з питань таємниць формувався «Звід відомостей, що становлять державну таємницю» (далі – ЗВДТ). Інститут державних експертів не існував в СРСР, не має його в інших країнах СНД. Щось подібне є в США – це так звані класифікатори 1-го рангу [18, с. 48].

Закон України «Про державну таємницю» вивів з обігу поняття «державні секрети» та розподілив інформацію, що віднесена до державної таємниці, на три ступені – «особливої важливості», «цілком таємно» та «таємно». Поняття «службова таємниця» та «державні секрети» в Законі не використовувалися. За радянських часів вважалося, що державні секрети – це всі ті відомості, які підлягають охороні з боку держави, бо їхнє розголошення може завдати шкоди державним інтересам. Державні секрети за ступенем секретності розподілялися на відомості «особой важности» і «совершенно секретные», які вважались державною таємницею, та «секретные» – службова таємниця. За замовчуванням усі носії інформації з грифом обмеження доступу «таємно», засекречені в СРСР та в незалежній Україні до прийняття 21 січня 1994 р. Закону України «Про державну таємницю» з грифами «секретно» і «таємно», перетворилися на носії інформації, що містять державну таємницю. Після прийняття Закону України «Про державну таємницю» ДКС України здійснив комплекс заходів, спрямованих на створення вітчизняної СОДТ. Найактуальнішою проблемою було формування відкритого загальнодержавного ЗВДТ України та персоніфікації цих дій. З цією метою ДКС України було розроблено «Положення про державного експерта з питань таємниць», затверджене Указом Президента України від 23 квітня 1994 р. № 185/94 [7].

Положення визначало, що державний експерт з питань таємниць у встановленому законом порядку здійснює віднесення інформації до державної таємниці, зниження ступеня секретності та скасування рішення про віднесення цієї інформації до державної таємниці, також було визначено права, обов'язки і відповідальність державних експертів з питань таємниць. До положення додавався перелік посад, на яких особи, що їх заміщують, виконують функції державних експертів з питань таємниць. Наведемо частину зазначеного переліку, а саме: посади генеральних та головних конструкторів науково-дослідних та конструкторських установ, які представляли АНТК імені Антонова (м. Київ), Харківське КБ машинобудування імені О. Морозова, КБ «Південне» (м. Дніпро), НВО «Хартрон» (м. Харків), НДІ «Квант» (м. Київ), НДІ комплексної автоматизації (м. Донецьк), ЦКБ «Протон» (м. Харків), Український радіотехнічний інститут (м. Миколаїв), ЦКБ ВО «Завод Арсенал» (м. Київ), НДПІ «Союз» (м. Харків), СКБ радіотехнічних пристроїв (м. Донецьк), НТК «Імпульс» (м. Київ), ДНДІ хімічної продукції (м. Шостка), КБ «Дніпровське» (м. Дніпро), Житомирський науково-дослідний інститут радіосистем, Національний науковий центр «Харківський фізико-технічний інститут». Усі інші посади, на яких особи, що їх заміщують, виконують функції державних експертів із питань таємниць, у зазначеному переліку представляли центральні державні органи влади [7].

Відповідно до «Положення про державного експерта з питань таємниць» були розроблені «Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності». Створення інституту державних експертів дозволило підняти експертні оцінки інформації, яка підлягала захисту, на державний рівень.

КМ України постановою від 29 квітня 1994 р. № 278 було затверджено «Положення про порядок і механізм формування та опублікування ЗВДТ». Положення встановлювало, що ЗВДТ є єдиною формою реєстрації відомостей, що становлять державну таємницю в Україні й з моменту опублікування ЗВДТ держава забезпечує захист і правову охорону відомостей, що в ньому зареєстровані.

Право формування ЗВДТ, внесення змін та доповнень до нього на підставі рішень державних експертів з питань таємниць було надано ДКС України. Реєстрація відомостей у ЗВДТ стала підставою для надання документу, виробу, іншому матеріальному носію інформації, що містить ці відомості, грифу секретності, який відповідає ступеню секретності, встановленому для них у ЗВДТ [7]. На попередньому етапі була здійснена робота зі створення 82 тимчасових переліків відомостей, що станов-

лять державну таємницю [19, арк. 120]. Після опублікування ЗВДТ державними органами на підставі та в межах ЗВДТ з метою конкретизації та систематизації інформації, яка віднесена до державної таємниці, були розроблені відомчі розгорнуті переліки відомостей, що становлять державну таємницю.

Такі переліки були погоджені з ДКС України і затверджені відповідними державними експертами з питань таємниць. Із дня опублікування ЗВДТ його вимоги стали обов'язковими для виконання суб'єктами України, діяльність яких пов'язана з державною таємницею. ДКС України наказом від 25 травня 1994 р. № 17 було створено робочу групу з організації та координації заходів з розробки нормативно-правового акту, який би повністю замінив Інструкцію № 0126-87 [20, арк. 26].

Закон України «Про державну таємницю» передбачав матеріальне стимулювання діяльності громадян, які постійно працюють з таємними відомостями, тобто за роботу в умовах режимних обмежень. Реалізація правової норми наведеної компенсації здійснювалася відповідним нормативним актом уряду.

Види, розміри і порядок надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці, були затверджені постановою КМ України від 15 червня 1994 р. № 414.

Ця постанова затверджувала правову норму щодо осіб, які працюють в умовах режимних обмежень. Таким особам встановлювалася надбавка до посадових окладів залежно від ступеня секретності інформації у такому розмірі: за роботу з відомостями «особливої важливості» – 20 %; «цілком таємно» – 15 %; «таємно» – 10 %. Особам, які працюють в умовах режимних обмежень і безпосередньо виконують таємні науково-дослідні та дослідно-конструкторські роботи, встановлювалася надбавка до посадових окладів залежно від ступеня секретності та обсягу інформації у такому розмірі: за роботу з відомостями «особливої важливості» – 70–100 %; «цілком таємно» – 30–70 %; «таємно» – 10–30 % [7]. Дія цієї постанови, на думку автора, має позитивний бік (заохочувальний) та негативний, оскільки це інколи призводило до збільшення обсягів таємних носіїв інформації, завищення їхнього ступеня секретності.

Важливою складовою СОДТ було розроблення і впровадження порядку і умов діяльності державних органів, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею. Постановою КМ України від 26 червня 1994 р. № 426 було затверджено «Положення про порядок і умови надання органам державної виконавчої влади, підприємствам, установам і організаціям дозволу (ліцензії) на здійснення діяльності, пов'язаною з державною таємницею, та про особливий режим цієї діяльності» [7]. Повноваження щодо ліцензування суб'єктів, діяльність яких пов'язана з державною таємницею, були надані ДКС України, який з другого півріччя 1994 р. розпочав цей процес.

Радикальне скорочення оборонних замовлень, конверсія науки й промисловості змінювали роль ВП в СОДТ, суттєво зменшивши сферу обігу таємної інформації, яка наповнювалась переважно структурами МО України та правоохоронними органами, які стали основним продуцентом таємниць. Разом з економіко-соціальними змінами в державі з'явились нові види інформації з обмеженим доступом, такі як банківська, комерційна й інші види таємної та конфіденційної інформації, яким за радянських часів надавався б статус службової таємниці. Нова незвична ситуація – відкриття кордонів та вільний рух інформації викликала занепокоєння у влади, оскільки це інколи призводило до певного небажаного витоку за кордон наукової, конструкторської документації тощо. На це зреагував і президент Л. Кучма, який виступаючи 27 липня 1994 р. перед співробітниками СБ України заявив, зокрема, таке: «[…] мені інколи здається, що в нас взагалі вже немає державних таємниць ні політичного характеру, ні військових, ні стосовно нових певних технологій і виробництв.

Ми не збираємося відновлювати «залізний щит» але зберігати свої державні таємниці потрібно, як і в будь-якій цивілізованій державі» [21, с. 4–5].

У 1994 р. почало зачинятися «вікно» можливостей для модернізації СОДТ: будь-які спроби нормопроектування за західними зразками зустрічали спротив. Усе поверталося до радянських лекал.

Так, 22 серпня 1994 р. спільним наказом Держкомтаємниць (не плутати з ДКС України) та Державної митної служби № 99/252 було затверджено «Інструкцію про порядок переміщення через державний кордон України текстових, аудіо- та аудіовізуальних матеріалів» [7], яка мала виразне радянське походження і була дуже схожа на Інструкцію НКВС № 001434 від 1939 р. [22, арк. 123–139] Згідно з цим документом від митників вимагалось: переглядати всі без винятку носії інформації, наприклад, зазначена інструкція дозволяла провозити через кордон тільки ті книги, журнали, художні альбоми, атласи, ноти, записи музичних творів, кінофільмів, що *не становлять історичної, наукової, художньої або іншої цінності* [курсив наш].

Заборонялося провозити матеріали з курсів військової підготовки, цивільної оборони і закритих спеціальностей, трудові книжки, видання з печатками діючих бібліотек і установ. Зазначена інструкція вимагала дозволу Урядової комісії з експортного контролю на перевезення через кордон: «відомостей або результатів науково-дослідних, дослідно-конструкторських робіт та дисертацій, які виконуються або були виконані на замовлення чи в інтересах оборони та безпеки України; друкованих матеріалів, рукописів, кліше, фото-, кіно-мате-

ріалів, відеозаписів, платівок та інших звукозаписів, малюнків, інших друкованих і образотворчих матеріалів, що містять відомості про зброю, військову чи спеціальну техніку або технології їх виготовлення; технічні засоби обробки та зберігання інформації, які мають енергонезалежні елементи пам'яті, магнітні диски та стрічки усіх видів, перфокарти та перфострічки тощо, що містять інформацію про зброю, військову чи спеціальну техніку або технології її виготовлення тощо». У зв'язку з відкриттям кордонів, за відсутності технологій та людських ресурсів, вказана інструкція майже не застосовувалася й була скасована у 2010 р.

Країна важко позбувалася радянських стереотипів. Наприклад, можна згадати таку курйозну зі сучасного погляду історію: в ті часи вже входив у наше життя Інтернет і між відомствами відбувалося листування щодо порядку погодження тексту е-мейлів з «компетентними органами» у термін за тиждень або місяць до їхнього відправлення за кордон.

Зрештою здоровий глузд переміг і нормативний акт про порядок візувань електронної пошти не був прийнятий.

КМ України постановою від 9 вересня 1994 р. № 632 було затверджено «Положення про технічний захист інформації в Україні» [6, с. 155–156]. Положенням було визначено порядок ТЗІ, що містить відомості, які становлять державну та іншу передбачену законом таємницю, конфіденційну інформації, що є власністю держави, а також інформацію обмеженого доступу, що є приватною власністю. Повноваження центрального органу державної виконавчої влади було покладено на ДС ТЗІ України. Наприкінці 1994 р. було прийнято постанову КМ України від 16 листопада 1994 р. № 779 «Про встановлення письмової форми трудових договорів з працівниками, діяльність яких пов'язана з державною таємницею».

Постанова встановлювала, що трудові договори з працівниками, діяльність яких пов'язана з державною таємницею, укладались у письмовій формі [7]. Повноцінно на практиці ця нормативна вимога не діяла і про неї швидко забули.

У 1994 р. на базі Міністерства інформації та Держкомтаємниць Указом Президента України від 18 листопада 1994 р. № 689/94 було створено Міністерство з питань преси та інформації України, за яким залишилися лише консультативні обов'язки щодо охорони таємниць у пресі та інших ЗМІ. Останній цензорський органу країні було ліквідовано [7].

Постановою ВР України від 28 листопада 1994 р. № 237/94-ПВ затвердили «Правила поводження народних депутатів України з таємними документами та інформацією» [23, арк. 149–157]. У 1994 р. почалося створення реєстру підприємств, установ і організацій, які виконували і виконують таємні державні замовлення для забезпечення потреб оборони і безпеки [17, арк. 29–52]. Наказом ДКС України від 8 грудня 1994 р. № 44 було введено в дію форму «Зобов'язання громадянина України у зв'язку з допуском до державної таємниці» [7].

15 грудня 1994 р. спільним наказом Міністерства охорони здоров'я України та ДКС України № 305/46 було затверджено перелік психічних захворювань, за наявності яких громадянин не може бути допущений до державної таємниці [7]. Національна система підготовки кадрів у РСО була започаткована створенням у жовтні 1994 р. на базі Національного технічного університету України «Київський політехнічний інститут» курсів підвищення кваліфікації спеціалістів РСО. У 1994 р. спільним рішенням СБ України і ДКС України повноваження цих державних органів були розмежовані юридично. Відповідно до законодавства СБ України продовжувала виконувати функції у СОДТ як спеціальний правоохоронний орган (контррозвідувальне забезпечення та перевірка громадян щодо допуску до державної таємниці).

Висновок

У 1991–1994 рр. в Україні СОДТ формувалася з урахуванням досвіду розвинених країн світу та традиційних засобів і методів, що виправдали себе у вітчизняній практиці.

Збільшилася відкритість держави перед суспільством, скоротилася чисельність відомостей, що належать до державної таємниці, відкритими стали загальні переліки такої інформації, механізми засекречування та умови розсекречування. Через різні обставини суттєво зменшилась кількість продуцентів таємної інформації та відповідно РСО.

Наприкінці першого півріччя 1993 р. було завершено створення державних органів, що забезпечували реалізацію державної політики у сфері охорони державної таємниці. Вжиті заходи в складних умовах початкового етапу державного будівництва дозволили створити логічну завершену організаційну структуру державних органів, діяльність яких була спрямована на формування і вдосконалення СОДТ України.

Література

[1] Ворожко В. Правові основи захисту інформації в Україні // *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Зб. доп.* – К., 1998. – С. 30−33.

[2] Ворожко В. З історії створення національної системи охорони державної таємниці // *Інформаційно-документальні комунікації в глобалізованому суспільстві: матеріали міжнар. наук.-прак. конф.* 21-22 березня 2013 р. – К.: НАУ, 2013. – С. 95−96.

[3] Ворожко В. З історії створення вітчизняної системи охорони державної таємниці. Травень 1993–січень 1994 рр. // *ITSec-2020: матеріали X міжнар. наук.-техн.*

конф. 19-24 березня 2020 р. – Київ, Шарм-ель-Шейх. – С. 50–52.

[4] Ворожко В. Перші кроки зі створення національної системи охорони державної таємниці. серпень 1991–травень 1993 рр. // *Безпека ресурсів інформ. систем: збірник тез І міжнар. наук.-прак. конф.* 16-17 квітня 2020 р. – Чернігів. – С. 72–78.

[5] *Охорона державних секретів незалежної України*. / Й. Мастяниця, Л. Шиманський, О. Олійник, В. Ворожко. − К.: Ін-т законодавства ВР України, 2010. – 128 с.

[6] Ворожко В. *Нарис історії охорони державної таємниці в Україні* / В. Ворожко, Б. Бернадський, О. Ботвінкін. – К.: Лазурит-Поліграф, 2012. – 188 с.

[7] *Законодавство України: Офіційний веб-сайт Верховної Ради України*. [Електронний ресурс] : http:// zacon.rada.gov.ua/cgi-bin/laws.

[8] *Галузевий державний архів Служби безпеки України* (ГДА СБ України), ф. 9, спр. 122-сп.

[9] Поровський М. Початки створення СБУ для захисту національної державності України // *Національна спецслужба в українському державотворенні: збір. статей і матеріалів з нагоди 29-ї річниці СБУ* / В. Омельчук та ін. – К.: Прометей, 2021. – С. 239–245.

[10] Скриник О. 10 років ГУУЗ – ДСТЗІ СБ України: Досягнення та перспективи // *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, 2002. – Вип. 5. – С. 7–8.

[11] Костенко Ю. Пригадуючи початок буремних 90-х…// *Національна спецслужба в українському державотворенні: збір. статей і матеріалів з нагоди 29-ї річниці СБУ* / В. Омельчук та ін. – К.: Прометей, 2021. – С. 234–236.

[12] Лопата А. *Записки начальника Генерального штабу Збройних сил України*. – К.: ВД «Воєнна розвідка», 2015. – 632 с.

[13] *Національна безпека України*, 1994–1996 рр.: наук. доп. НІСД – К.: НІСД, 1997. − 197 с.

[14] *Центральний державний архів вищих органів влади України*, ф. 5282, оп.1, спр. 1.

[15] Ворожко В., Пащенко О. Стан розсекречування архівних документів у сучасній Україні. // *Студії з архів. справи та документознавства*. – 2010. – Т. 18. – С. 32–37.

[16] Ворожко В., Муратов О. Засекречування відомостей в США. Історія і сучасність / *Воєнно-історичний вісник*. – 2013. – Вип. 3 (9). – С. 22–33.

[17] *Центральний державний архів вищих органів влади України*, ф. 5282, оп.1, спр. 7.

[18] Ворожко В. Система засекречивания и рассекречивания в США // *Безопасность информации*. – 1997. – № 1 (8). – С. 48–53.

[19] *Центральний державний архів вищих органів влади України*, ф. 5282, оп. 1, спр. 10,

[20] *Центральний державний архів вищих органів влади України*, ф. 5282, оп. 1, спр. 5

[21] *Галузевий державний архів Служби безпеки України* (ГДА СБ України), ф. 68, спр. 13.

[22] *Галузевий державний архів Служби безпеки України* (ГДА СБ України), ф. 9, спр. 10-сп.

[23] *Центральний державний архів вищих органів влади України*, ф. 5282, оп. 1, спр. 18.

Vorozhko ***V. The establishment of the ukrainian system of state secret protection. 1991–1994***

Abstract. *The article examines the formation of state bodies of Ukraine responsible for information security, creation of a system of protection of state secrets, government communications, technical protection of information with limited access in 1991-1994 based on legislative acts of Ukraine, works of Ukrainian researchers and archival documents of the Central State Archives of Ukraine. Particular attention is paid to the regulations of Ukraine on the protection of state secrets and the activities of the State Committee of Ukraine for State Secrets. The author analyzes: the current situation related to the secrets of the military industry and the military department, inherited from the former Soviet Union and the Agreement of post-Soviet countries on mutual protection of interstate secrets; systematized carriers of classified information in circulation or stored at the time in regime-secret bodies; the comparison of the Soviet and Ukrainian systems of protection of state secrets; the process of forming the first Ukrainian code of information containing state secrets. The researcher also conducts a comparative analysis of the functions of the State Secretariat of Ukraine and the Security Service of Ukraine and the relative US government agencies, such as the Office of Information Security (ISOO) and the Federal Bureau of Investigation (FBI). The paper considers the role of the Ukrainian institute of "state experts on secrets" and problematic issues of material incentives for citizens to work under regime restrictions. The author provides examples of relict remnants of Soviet censorship and the transformation of Ukrainian censorship bodies. The research methodology is based on the principles of objectivity, positivism, systematics, historicism, and the following historical methods: problem-chronological, historical-comparative, historical-legal.*

Keywords*: The State Committee of Ukraine for State Secrets, Security Service of Ukraine, SODT, classified information, classified documents, technical protection of data, government relations.*

Ворожко В.П. Становление Украинской системы охраны государственной тайны. 1991–1994

Аннотация*. В статье на основе законодательных актов Украины, работ украинских исследователей и архивных документов ЦДАВО Украины рассматриваются процессы формирования государственных органов Украины, ответственных за информационную безопасность, создания системы охраны государственной тайны, правительственной связи, технической защиты информации с ограниченным доступом в 1991–1994 гг.; особое внимание уделено нормативно-правовым актам Украины по защите государственной тайны и деятельности*

Государственного комитета Украины по вопросам государственных секретов. Автором проанализированы: состояние носителей с тайнами военной промышленности и военного ведомства, оставшихся в наследство от бывшего СССР, а также Соглашение постсоветских стран о взаимном обеспечении сохранности межгосударственных секретов. Систематизированы носители секретной информации, находившиеся в то время в обращении или на хранении в режимно-секретных органах. Сделан сравнительный анализ советской и украинской систем охраны государственной тайны. Исследован процесс формирования первого украинского Свода сведений, содержащих государственную тайну. Проведен сравнительный анализ функций Госкомсекретов Украины и Службы безопасности Украины с функциями государственных органов США, ответственных за охрану государственных тайн, таких как Управление по надзору за информационной безопасностью (ISOO) и Федерального бюро расследований (FBI). Рассмотрены функции украинского института «государственных экспертов по вопросам тайн» и проблемные вопросы материального стимулирования граждан за работу в условиях режимных ограничений. Приведены примеры реликтовых остатков советской цензуры и рассмотрен процесс трансформации цензорских органов Украины. Методология исследования опирается на принципы объективности, позитивизма, системности, историзма и базируется на исторических методах: проблемно-хронологическом, историко-сравнительном, историко-правовом.

***Ключевые слова**. Госкомсекретов, СБ Украины, СОДТ, секретные сведения, секретные документы, техническая защита информации, правительственная связь.*

Ворожко Валерій Павлович-кандидат історичних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету; провідний науковий сотрудник Отраслевого державного архіву Служби безпеки України.

Ворожко Валерий Павлович – кандидат исторических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета; ведущий научный сотрудник Отраслевого государственного архива Службы безопасности Украины.

Valeriy Vorozhko – PhD, Associate Professor, Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine); leading researcher of Security Service of Ukraine State Archives Branch.

Отримано 21 *червня 2021 року,* затверджено редколегією *27 серпня 2021 року*

ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

DOI: 10.18372/2225-5036.27.16005

РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ ТА ЯКІСТЬ ПІДГОТОВКИ СПЕЦІАЛІСТІВ З КІБЕРБЕЗПЕКИ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ УКРАЇНИ ЯК ПЕРЕДУМОВА УЧАСТІ В ДЕРЖАВНИХ ПРОГРАМАХ СПРИЯННЯ РОЗВИТКУ ОСВІТНЬОЇ СПЕЦІАЛЬНОСТІ

Потій Олександр Володимирович, д. т. н., професор,

Рік та місце народження: 1971 р., м. Кривий Ріг, Україна
Освіта: Харківське вище військове командно-інженерне училище ракетних військ
Посада: заступник Голови Державної служби спеціального зв'язку та захисту інформації України
Наукові інтереси: комп'ютерна безпека, криптографія, кібербезпека критичної інфраструктури, вища освіта, бізнес-інформатика
Публікації: більше 150 наукових публікацій у галузі інформаційної, кібербезпеки, криптографії, серед яких наукові статті, монографії, підручники та навчально-методичні посібники, патенти на корисні моделі
E-mail: potav1971@gmail.com.
Orcid ID: 0000-0002-2366-0541.

Бакалинський Олександр Олегович, к. т. н.

Рік та місце народження: 1970 р., м. Київ, Україна
освіта: Київський військовий інститут управління та зв'язку, Національна академія Служби безпеки України
Посада: заступник директора Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України
Наукові інтереси: системи управління інформаційною безпекою, управління ризиками, кібербезпека критичної інфраструктури, вища освіта
Публікації: Більше 60 наукових публікацій у галузі інформаційної, кібербезпеки, серед яких наукові статті, монографії, підручники та навчально-методичні посібники, патенти на корисні моделі
E-mail: baov@meta.ua.
Orcid ID: 0000-0001-9712-2036.

Мялковський Данило Владиславович, к. д. у.

Рік та місце народження: 1971 р., м. Київ, Україна.
Освіта: Київський військовий інститут управління та зв'язку, Національна академія державного управління при Президентові України.
Посада: директор Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України.
Наукові інтереси: державне управління у сфері кібербезпеки, захисту інформації, безпеки електронних послуг.
Публікації: Більше 20 наукових публікацій, серед яких 12 наукових статей, в тому числі 4, виданих в іноземних наукових виданнях.
E-mail: daniilvm71@gmail.com.
Orcid ID: 0000-0002-8246-8437.

Верба Денис Володимирович, к.е.н., доцент

Рік та місце народження: 1974 р., м. Київ, Україна.
Освіта: Київський національний економічний університет імені Вадима Гетьмана.
Посада: доцент ДВНЗ «КНЕУ імені Вадима Гетьмана».
Наукові інтереси: економіка соціальної сфери, оцінювання державних програм та політики.
Публікації: більше 60-ти наукових публікацій, серед яких наукові статті, монографії, підручники та навчально-методичні посібники.
e-mail: denys.verba@kneu.ua.
Orcid ID: 0000-0002-8712-4027.

Анотація. *Стаття присвячена огляду передумов, що вітчизняні заклади вищої освіти (ЗВО), де ліцензована спеціальність 125 «Кібербезпека», мають для якісної підготовки спеціалістів відповідної кваліфікації у зв'язку з характеристикою якості підготовки (позицією ЗВО у консолідованому рейтингу українських вишів). До таких передумов віднесені масштаби освітньої діяльності ЗВО; їх спеціалізація; відповідність спеціалізації кафедри набору компетенцій, що набувають випускники спеціальності 125 «Кібербезпека»; забезпеченість освітнього процесу викладачами з кандидатським і докторським ступенем. Визначені агреговані, придатні для порівняння оцінки ресурсного потенціалу ЗОВ для якісної підготовки фахівців з кібербезпеки та показники рівня використання такого потенціалу. За результатами 56 ЗВО, де готують фахівців з кібербезпеки розподілено на чотири групи. До першої групи віднесені ЗВО, що обіймають провідні позиції як за наявністю передумов якісної підготовки фахівців з кібербезпеки, так і за оцінкою якості підготовки. До другої групи увійшли ЗВО, що мають вищі за середні, але не кращі показники передумов якісної підготовки фахівців з кібербезпеки, і високі показники якості підготовки: таке позиціювання свідчить про успішну реалізацію середнього і високого потенціалу. До третьої групи увійшли ЗВО, що обіймають високі позиції в рейтингу якості підготовки, маючі гірші медіанних передумови якісної підготовки фахівців з кібербезпеки. Нарешті, до четвертої групи увійшли ЗВО, що за наявними даними не мають достатніх передумов для якісної підготовки фахівців з кібербезпеки, що підтверджується позицією ЗВО в консолідованому рейтингу українських вишів.*

Ключові слова*: освіта, кібербезпека, кадрове забезпечення, вища освіта, якість підготовки.*

Постановка проблеми

Наявний потенціал закладів вищої освіти України щодо підготовки спеціалістів з кібербезпеки (125-та спеціальність «Кібербезпека» за Постановою КМУ від 29 квітня 2015 р. [1]) є однім з ключових факторів забезпечення високого рівня інформаційної безпеки, як для комерційних установ, так і для органів державної влади. Відповідно, суспільні вимоги до функціонування цього сегменту освіти, формуються на перетині складної та суперечливої системи економічних, соціальних, техногенно-безпекових критеріїв.

Це актуалізує цілу низку завдань щодо науково-аналітичного обґрунтування державного сприяння розвитку освіти з кібербезпеки.

Зокрема, розробку інформаційно-аналітичного обґрунтування системи пріоритетів і завдань державної політики розвитку освіти з кібербезпеки, що відповідатиме як потребам основних стейкхолдерів освіти відповідного напряму, так і стратегічним завданням державних програмних документів з кібербезпеки, розвиваючи та уточнюючи концептуальні положення публікацій, присвячених розробці організаційно-технічної моделі кіберзахисту [2 – 6].

Важливою складовою такого обґрунтування є дослідження, присвячені зіставленню накопиченого в певних освітніх центрах кадрового та ресурсного потенціалу з характеристиками результатів його застосування – масштабами та якістю підготовки.

Результати таких досліджень забезпечують класифікацію освітніх установ, що здійснюють підготовку кадрів з кібербезпеки за ознакою наявності (вираженості) передумов для ефективної участі в державних програмах розвитку освіти, спроможності ефективно долучатись до державно-приватного партнерства для вирішення завдань кадрового забезпечення діяльності з протидії кіберзагрозам національній безпеці України.

Аналіз останніх досліджень і публікацій

Проблематика цієї статті перебуває на перетині двох напрямів наукових досліджень, що мають вагомий спільний сегмент об'єкту дослідження, проте відрізняються предметом і, відповідно, концептуальними підходами та інструментарієм. До першого напряму можна віднести дослідження, що сконцентрованості на організаційно-правових аспектах функціонування сектору вищої освіти спеціальності «кібербезпека» та розглядають принципи регламентації та доцільні процедури забезпечення дотримання регламентів відносин між освітніми закладами, споживачами освітніх послуг, роботодавцями, державою для досягнення ефективного компромісу специфічних інтересів за дотримання вимог та пріоритетів забезпечення національної кібербезпеки [7 – 10]. В складі другого напряму з певною умовністю, можна об'єднати дослідження соціально-економічних аспектів функціонування освіти та, зокрема, сегментів вищої освіти певного професійного спрямовування [11 – 16]. В контексті нашого дослідження, концептуальні положення обох цих напрямів будуть застосовані щоб сформулювати та випробувати на вітчизняних статистичних показниках, підходи до обґрунтування соціально-економічних аспектів створення моделі кібеззахисту України. Зокрема, в роботі [6], виділяються головні цілі створення організаційно-технічної моделі кіберзахисту, серед яких першою названа «підвищення ефективності функціонування національної системи кібербезпеки та посилення координації дій, що здійснюються суб'єктами кіберзахист». Також серед цілей створення ОТМ виділяється «створення умов для розвитку державно-приватного партнерства в інтересах кіберзахисту критичної інфраструктури». Власне підвищенню ефективності використання ресурсного потенціалу сегменту вищої освіти, де готуються кадри за спеціальністю 125 «Кібербезпека» це дослідження сприятиме завдяки розробці системи критеріїв та показників для оцінки наявності (вираженості) у окремих освітніх центрів передумов

ефективної участі в програмах державного сприяння розвитку освіти за відповідною спеціальністю.

Водночас, розробка такого інструментарію сприятиме і розвитку державно-приватного партнерства, зокрема завдяки поліпшенню обґрунтованості (комплексності врахування соціально-економічного ефекту від використання обмежених ресурсів, виділених суспільством на цілі поліпшення кадрового забезпечення кіберзахисту в межах окремих центрів підготовки кадрів) та прозорості вибору Закладу вищої освіти (ЗВО) для участі в державних програмах сприяння розвитку освіти зі спеціальності 125 «Кібербезпека».

Відповідно, аналітичне позиціювання ЗВО, за наявністю ознак готовності забезпечувати високу ефективність участі в державних програмах розвитку вищої освіти за 125-ою спеціальністю і є метою цього дослідження.

Це має створити інформаційні передумови для прозорого та відповідного пріоритетам і завданням розвитку академічного сектору організаційно-керівної інфраструктури кіберзахисту [6] відбору конкретних освітніх центрів для виконання ролі опорних освітніх хабів, чи структурних ланок мережі освітніх закладів, долученої до функціонування національної моделі кіберзахисту.

Виклад основного матеріалу

Концепція дослідження ґрунтується на таких базових тезах.

1. Структура мережі закладів вищої освіти (далі – ЗВО), що здійснюють підготовку бакалаврів та магістрів за 125-ою спеціальністю є важливим фактором забезпеченості потреб суспільства у професіоналах відповідної кваліфікації.

2. Різноманітність центрів підготовки фахівців (за масштабами діяльності ЗВО, їхнім статусом, спеціалізацією, формою власності, регіональною належністю) та розпорошеність загальних обсягів підготовки є необхідною умовою задіяння конкурентних факторів розвитку відповідного сектору освітніх послуг, забезпечення можливостей доступу до освітніх послуг для різних верств населення та досягнення відповідності пропозиції і попиту на освітні послуги за спеціальністю 125 «Кібербезпека».

3. Водночас, розмаїття навчальних закладів та програм посилює важливість стандартизації компетенцій, одержуваних студентами в межах державного замовлення, актуалізує потребу у створенні провідних центів підготовки, що задаватимуть вищі стандарти якості освітніх послуг, виконуватимуть роль «лідерів» та провідників розвитку освітніх технологій.

4. Виділення таких провідних центрів підготовки бакалаврів та магістрів, за спеціальністю 125 «Кібербезпека» має враховувати результати прозорої конкуренції, вільного волевиявлення студентів, викладачів, роботодавців, всіх стейкхолдерів освітнього процесу, взаємодія яких забезпечує поступове виділення лідерів в сегменті освіти за названою спеціальністю.

Відповідно, характеристики масштабів підготовки, забезпеченості навчального процесу провідними викладачами, успіхи у міжнародному співробітництві мають розглядатись як знаки здатності ЗВО забезпечити високу ефективність участі в державних програмах розвитку. Для оцінки та рейтингування (позиціювання) ЗВО, які здійснюють підготовку бакалаврів та магістрів за спеціальністю 125 «Кібербезпека» використовуються два критерії.

Перший – масштаби діяльності, оскільки ми вважаємо, що більші масштаби діяльності, як прояв популярності серед студентів, ознака здатності концентрувати кращі викладацькі кадри, слугують передумовою готовності ЗВО забезпечити високу ефективність участі в державних програмах підтримки і розвитку освіти за спеціальністю 125 «Кібербезпека».

Другий – відповідність спеціалізації ЗВО та випускаючої кафедри набору компетенцій, що одержують випускники спеціальності 125 «Кібербезпека» , оскільки ми вважаємо, що саме наявність у ЗВО кадрових, методичних та ресурсних можливостей для здійснення підготовки відповідно до спеціальності 125 «Кібербезпека», а також для підготовки за спорідненими спеціальностями (зокрема 123 «Комп'ютерна інженерія» та 124 «Системний аналіз»), дозволятиме одержувати додатковий ефект від державної підтримки завдяки синергетичному ефекту від взаємопідтримуючого розвитку споріднених спеціальностей.

Для характеристики масштабів діяльності використовуються показники чисельності студентів ЗВО (показник масштабів діяльності ЗВО), чисельність докторів та кандидатів наук, зайнятих в штаті випускаючої кафедри спеціальності 125 «Кібербезпека»та ліцензовані обсяги прийому бакалаврів і магістрів за цією спеціальністю (як показники масштабів освітньої діяльності в межах спеціальності). Також враховуються позиція ЗВО в структурі регіональних філій (наявність / відсутність відокремлених структурних підрозділів, здатних забезпечувати попередню підготовку та відбір абітурієнтів та статус відносно таких підрозділів – чи є ЗВО головною установою, чи сам є складовою підпорядкованої регіональної структури. Для характеристики відповідності спеціалізації ЗВО та випускаючої кафедри профілю спеціальності 125 «Кібербезпека» враховується спеціалізація ЗВО та кафедри. Наведений перелік показників не враховує низку показників якості освітнього процесу (зокрема, залученість студентів до наукової роботи та виконання досліджень за договорами кафедри, якість організації практики, перспективи працевлаштування та інші, здатні

суттєво уточнити характеристики якості й результативності освітнього процесу) проте розширення такого переліку та розробку процедур отримання і верифікації такої інформації ми вважаємо важливим завданням подальших досліджень.

Для одержання порівнюваних та придатних до агрегування (розрахунку одного узагальнюючого показника) використана поширена формула нормування різних за розмірністю показників. Для показників, збільшення розмірів яких тлумачиться як ознака зростання потенціалу ЗВО щодо забезпечення високої якості підготовки:

$$EVAL_i = \frac{F_i - F_{min}}{F_{max} - F_{min}} \times 100. \quad (1)$$

Для показників, щодо яких менший абсолютний розмір тлумачиться як ознака зростання потенціалу ЗВО щодо забезпечення високої якості підготовки:

$$EVAL_i = \frac{F_{max} - F_i}{F_{max} - F_{min}} \times 100, \quad (2)$$

де:

$EVAL_i$ – оцінка «і-го» ЗВО;

F_i – значення нормованого показника для «і-го» ЗВО;

F_{max} – максимальне значення нормованого показника серед всіх оцінюваних ЗВО;

F_{min} – мінімальне значення нормованого показника серед всіх оцінюваних ЗВО.

Наведені формули досить поширені для порівняльного оцінювання характеристик суспільних процесів, що надалі агрегуються в складі комплексних показників (наприклад, застосовуються для розрахунку компонентів індексів людського розвитку [17]) і дозволяють відобразити співвідношення між значеннями показників різних ЗВО у вигляді бальної оцінки від «0» (гірше серед всіх ЗВО значення) до «1» (краще серед всіх ЗВО значення.

Для оцінки ознак досягнутого рівня якості підготовки використовується позиція ЗВО в консолідованому рейтингу ЗВО України, який враховує позицію в «ТОП 200 Україна», кількість та цитованість публікацій викладачів ЗВО у виданнях, що індексуються "SCOPUS" та середній бал абітурієнтів, зарахованих на контракт в межах вступної компанії 2020 р. Підготовку бакалаврів та магістрів за спеціальністю 125 «Кібербезпека» в Україні здійснюють56 ЗВО (за даними Міносвіти, [18]). Характеристики масштабів діяльності ЗВО, їх спеціалізації, забезпеченості кадрами вищої кваліфікації радикально диференційовані. Так, комплексний показник якості підготовки (позиція в консолідованому рейтингу ЗВО України 2020р.) коливається від нижчої (241-ої серед 241 ЗВО, включених до рейтингу) до 1-ої, яку обіймає Київський національний університет імені Тараса Шевченка (тут і далі – за даними аналізу інформації з відкритих джерел, переважно – сайтів ЗВО та сайтів домену osvita.ua, адміністрація яких несе відповідальність за достовірність наведених даних).

Загальна чисельність студентів ЗВО Показник наявності переваг щодо масштабів освітньої діяльності, оцінений за коливається від 223 (у Вінницькому навчально-науковому центрі Одеської національної академії зв'язку ім. О.С. Попова) до 33000 (Національний університет «Львівська політехніка»). Ліцензовані обсяги за 125-ою спеціальністю на бакалаврському рівні підготовки коливаються від 585 до 15, а на магістерському – від «0» до 257. Перша серія наведених нижче таблиць ілюструє зв'язок нормованих оцінок загальної чисельності студентів і якості підготовки (позиції в консолідованому рейтингу ЗВО). Бачимо, що для першої десятки ЗВО (табл. 1.а) з найчисельнішим контингентом студентів властиві досить різнорідні позиції в списку за якістю підготовки: серед них як ті, хто посідають місця в першій десятці (таких 5-ть), так і ті, що обіймають позиції в другому, третьому, четвертому та п'ятому десятку. Якщо середній рейтинг першої десятки найбільших ЗВО за чисельністю студентів 5,5, то ті самі ЗВО за якістю підготовки мають середній рейтинг 15,2 (майже в три рази гірший). Це свідчить, що великі масштаби підготовки самі по собі не є достатньою умовою провідних позицій щодо її якості, хоча явно замалі масштаби ЗВО вкрай знижують вірогідність високої якості підготовки завдяки складності набрати у достатній чисельності висококваліфікований науково-педагогічний персонал при умовах виконання вимог Постанови КМУ №1134 від 17 серпня 2002 р «Про затвердження нормативів чисельності студентів (курсантів), аспірантів (ад'юнктів), докторантів, добувачів наукового ступеня кандидата наук, слухачів, інтернів, клінічних ординаторів на одну штатну посаду науково-педагогічного працівника у вищих навчальних закладах III і IV рівня акредитації та вищих навчальних закладах післядипломної освіти державної форми власності» в якій встановлюється залежність кількісті викладачів ЗВО пропорційно кількості набраних студентів. Так, в табл. 1.б наведені дані по шістнадцяти ЗВО з найменшою чисельністю студентів – саме серед них сконцентровані й, переважно, аутсайдери консолідованого рейтингу з якості підготовки.

Про це свідчить близькість середніх рейтингів по чисельності студентів та якості підготовки: 45,5 для п'ятої десятки ЗВО за численністю студентів та 42,2 – за якістю підготовки. 51,8 середній рейтинг для останніх шести ЗВО за чисельністю студентів і 48 – середній рейтинг за якістю підготовки. Поки випробовуючи пілотний варіант методичних підходів до позиціювання, ми не враховуємо специфіку військових ЗВО, де діють особливі фактори співвідношення чисельності викладачів і студентів, проте плануємо врахувати специфіку таких ЗВО в подальших дослідження. Отже, великі масштаби

підготовки (провідні позиції за чисельністю студентів) самі по собі не гарантують високої якості підготовки, проте серед ЗВО, що не досягли певного необхідного масштабу діяльності явно домінують і нижчі стандарти якості підготовки. В межах нашого дослідження виявлено всього два виключення із наведеного вище правила (найменші масштаби діяльності поєднуються з низькими позиціями в рейтингу якості підготовки а серед ЗВО з найбільшою чисельністю студентів. Для оцінки передумов високої ефективності участі ЗВО в державних програмах розвитку освіти за 125-ою спеціальністю, враховано також масштаби підготовки бакалаврів та магістрів за цією спеціальністю (ліцензовані обсяги прийому). Щодо цієї характеристики важко очікувати наявності безпосереднього зв'язку з показниками якості підготовки для усього ЗВО (такий зв'язок може існувати з якістю підготовки в межах однієї спеціальності, або групи споріднених спеціальностей/ галузі). Проте за додаткового припущення про досить рівну якість підготовки за різними спеціальностями в межах ЗВО ми можемо розглядати позицію ЗВО в рейтингу якості підготовки, як характеристику якості підготовки за спеціальністю. Відповідно, зведення нормованих оцінок та рейтингів ЗВО за ліцензійними обсягами та якістю освіти наведено для 15-ти ЗВО з найбільшими обсягами підготовки за 125-ою спеціальністю в табл. 2.

Наведені дані свідчать, що ліцензовані обсяги переважної більшості ЗВО радикально відрізняються від нечисельної групи «лідерів».

Так беззаперечний лідер (Національний авіаційний університет) з сумарним ліцензованим обсягом бакалаврату і магістратури 815 (бальна оцінка «100») випереджає найближчий до нього за ліцензованими обсягами ЗВО (Державний університет телекомунікацій) майже на 30%. Крім цього, ще лише чотири ЗВО відстають за ліцензованими обсягами приблизно вдвічі. Всі інші ЗВО мають ліцензовані обсяги мінімум в три рази менші ніж ЗВО «лідер».

Таблиця 1.а

Масштаби та якість підготовки для найбільших ЗВО

Позиція ЗВО у рейтингу за масштабами діяльності	Бальна оцінка масштабів діяльності ЗВО, від «0» - найменша чисельність до «100» - найбільша чисельність	якість підготовки для ЗВО	
		Бальна оцінка, від «0» до «100»	Ранг серед 56 ЗВО
1	100,00	97,50	5
2	90,85	99,38	2
3	84,75	71,67	31
4	75,59	0,00	50
5	75,59	100,00	1
6	72,54	86,67	17
7	63,61	98,75	3
8	60,34	80,83	23
9	48,13	88,33	16
10	48,13	98,33	4

Таблиця 1.б

Масштаби та якість підготовки для найменших ЗВО

Позиція ЗВО у рейтингу за масштабами діяльності	Бальна оцінка масштабів діяльності ЗВО, від «0» - найменша чисельність до «100» - найбільша чисельність	якість підготовки для ЗВО	
		Бальна оцінка, від «0» до «100»	Ранг серед 56 ЗВО
41	13,78	75,83	28
42	13,05	35,21	43
43	10,91	33,75	45
44	9,30	62,50	37
45	9,08	34,58	44
46	8,47	22,71	48
47	6,95	2,08	49
48	4,33	50,00	40
49	2,91	59,17	38
50	2,00	0,00	50
51	0,54	43,96	41
52	0,00	0,00	50
52	0,00	0,00	50
52	0,00	0,00	50
52	0,00	31,25	47
52	0,00	0,00	50

Таблиця 2

Ліцензовані обсяги та якість підготовки для ЗВО з найбільшими ліцензованими обсягами прийому за 125-ою спеціальністю

Ранг за ліцензованими обсягами підготовки	Бальна оцінка ліцензованих обсягів підготовки	Якість підготовки за спеціальністю	
		Бальна оцінка	Ранг за якістю підготовки
1	100,00	88,33	16
2	72,02	50,00	40
3	50,92	97,50	5
4	46,01	88,75	15
5	45,40	86,04	18
6	42,33	95,63	6
7	33,13	58,75	39
8	28,34	99,38	2
9	25,15	2,08	49
10	21,47	36,46	42
11	18,40	72,29	29
12	16,20	86,04	18
13	15,34	80,00	24
14	13,50	77,50	26
15	12,27	0,00	50

Таблиця 3.а

Чисельність викладачів з науковим ступенем в штаті випускаючої кафедри спеціальності 125 і якість підготовки

Ранг ЗВО за чисельністю викладачів з науковим ступенем	Бальна оцінка чисельності викладачів із науковим ступенем	Відношення чисельності викладачів до ліцензійних обсягів		Якість підготовки за спеціальністю	
		Бальна оцінка	Ранг за забезпеченістю кадрами ліцензованих обсягів	Бальна оцінка	Ранг за якістю підготовки
1	100,00	22,12	15	95,63	6
2	52,05	4,87	32	88,33	16
3	49,32	75,27	3	90,42	13
4	46,58	78,99	2	91,04	12
5	30,14	100,00	1	82,50	21
6	28,77	16,63	22	86,04	18
6	28,77	9,50	28	99,38	2
8	26,03	7,36	30	58,75	39
8	26,03	49,66	5	32,29	46
10	23,29	22,22	14	94,17	9
11	21,92	9,56	27	36,46	42
11	21,92	18,59	17	33,75	45
13	19,18	36,59	6	43,96	41
13 (14)	19,18	58,55	4	0,00	50
13 (15)	19,18	18,30	18	92,08	11

Проте стосовно якості підготовки такої диференціації не спостерігається: в першій за ліцензованими обсягами п'ятірці ЗВО переважають рейтинги з другої десятки. Якщо середній рейтинг для першої п'ятірки за ліцензованими обсягами «3», то ці ж ЗВО мають середній рейтинг за якістю підготовки 18,8 – значно нижчий.Так само, диференційована якість підготовки і в інших ЗВО з найбільшими ліцензованими обсягами: великі ліцензовані обсяги за спеціальністю не виступають надійною гарантією високої якості підготовки. ЗВО і з першої (кращої), і з остатньої (гіршої) десятки за якістю підготовки присутні і в першій, і в останній десятці за ліцензійними обсягами. Так само і стосовно ЗВО, розташованих в середині рейтингу за розмірами ліцензованих обсягів прийому не спостерігається кореляції між рангами ЗВО за ліцензованими обсягами і якістю підготовки.

Третій показник врахований для оцінки передумов високої ефективності участі ЗВО в державних програмах розвитку освіти за 125-ою спеціальністю – чисельність докторів і кандидатів наук, зайнятих на випускаючих кафедрах ЗВО. Первинні дані доповнені розрахунковим показником, оскільки чисельність працюючих в штаті випускаючої кафедри кандидатів і докторів наук характеризує забезпеченість навчального процесу кадрами не самі по собі, а у відношенні до чисельності студентів, які навчаються за спеціальністю.

Тому для характеристики забезпеченості навчального процесу кадрами розраховано також відношення чисельності докторів і кандидатів наук до ліцензійних обсягів прийому: скільки викладачів з науковим ступенем припадатиме на одного студента першокурсника за повної реалізації ліцензійних обсягів. П'ятнадцять ЗВО з найбільшою чисельністю викладачів з науковим ступенем, працюючих в штаті випускаючої кафедри за 125-ою спеціальністю (табл. 3.а) переважно, мають не найвищі ранги за як за відношенням чисельності викладачів з науковим ступенем до ліцензованих обсягів, так і за якістю підготовки. Зокрема, з 15-ти відібраних ЗВО лише близько третини належать до першої десятки за забезпеченістю кадрами ліцензованих обсягів (шість ЗВО) і лише 20% (три ЗВО) мають високі рейтинги за якістю підготовки. Переважна частка ЗВО з 15-ти тих, де на випускаючій кафедрі найбільше викладачів з науковим ступенем, мають посередні позиції в рейтингу якості навчання: вони належать до другої, третьої, четвертої та навіть п'ятої десятки у рейтингу якості підготовки. Так рейтинги нижче 40-го за якістю підготовки мають п'ять з п'ятнадцяти відібраних ЗВО.

Таблиця 3.б

Забезпеченість викладачами з науковим ступенем ліцензованих обсягів спеціальності 125 і якість підготовки

Ранг ЗВО за забезпеченістю кадрами ліцензованих обсягів	Бальна оцінка відношення чисельності викладачів до ліцензійних обсягів	Чисельність викладачів із науковим ступенем		Якість підготовки за спеціальністю	
		Бальна оцінка	Ранг за чисельністю викладачів	Бальна оцінка	Ранг за якістю підготовки
1	100,00	30,14	5	82,50	21
2	78,99	46,58	4	91,04	12
3	75,27	49,32	3	90,42	13
4	58,55	19,18	13	0,00	50
5	49,66	26,03	8	32,29	46
6	36,59	19,18	13	43,96	41
7	33,98	17,81	16	67,50	33
8	31,36	8,22	33	35,21	43
9	29,87	13,70	21	72,29	29
10	27,88	10,96	26	59,17	38
10	27,88	10,96	26	0,00	50
10	27,88	5,48	40	34,58	44
13	25,09	16,44	18	89,58	14
14	22,22	23,29	10	94,17	9
15	22,12	100,00	1	95,63	6

Переважання за показником забезпеченості викладацькими кадрами ліцензованих обсягів прийому також не має вираженого зв'язку з перевагами за якістю підготовки (табл. 3.б). Серед п'ятнадцяти ЗВО з кращою забезпеченістю переважають ЗВО з другої, третьої, четвертої десятки за рейтингу за якістю навчання. Крім того, і серед ЗВО з найменшою чисельністю викладачів з науковим ступенем в розрахунку на одиницю ліцензованих обсягів присутні ЗВО, що мають досить високий рейтинг за якістю підготовки.

Для узагальнюючого позиціювання ЗВО за передумовами ефективної участі в державних програмах розвитку освіти за 125-ою спеціальністю розраховано інтегральний показник, що враховує як бальну оцінку масштабів діяльності ЗВО (чисельності студентів), так і оцінку масштабів підготовки за спеціальністю (ліцензовані обсяги), так і кадрове забезпечення навчального процесу (чисельність викладачів).

При цьому, показник масштабів діяльності ЗВО зважено на коефіцієнт, що відображає відповідність спеціалізації ЗВО змісту підготовки випускників 125-ої спеціальності (коефіцієнт дорівнює «1» для національних технічних ЗВО, «0,8» – для національних університетів універсальної спеціалізації, 0,7 – для університетів гуманітарної спеціалізації). Показник масштабів підготовки за спеціальністю зважується на коефіцієнт, що відображає відповідність спеціалізації випускаючої кафедри набору компетенцій, що набувають випускники спеціальності 125 (від 0,8 до 1). Таке позиціювання відображає загальну залежність якості підготовки у ЗВО (оцінена за його позицією в консолідованому рейтингу українських ЗВО) від наявності переваг масштабу та спеціалізації. Результати позиціювання наведені на рис. 1. Вони дозволяють класифікувати всі 56 включених до дослідження ЗВО на три групи.

До першої групи віднесені ЗВО, що обіймають провідні позиції як за наявністю передумов ефективності участі в державних програмах розвитку освіти (мають найвищі оцінки наявних переваг масштабів діяльності та спеціалізації), так і за оцінкою якості підготовки (найвищі позиції в консолідованому рейтингу українських ЗВО). Таке лідерство виражає очікувану реалізацію наявного потенціалу у високих показниках якості підготовки.

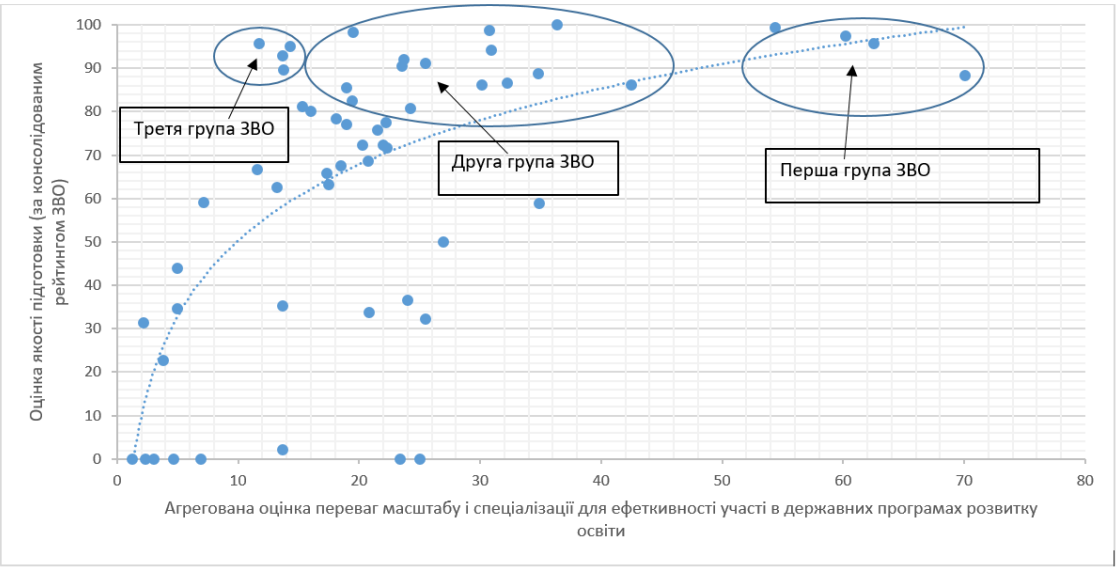


Рис. 1. Позиціювання ЗВО за перевагами масштабу та спеціалізації та якістю підготовки

До другої групи увійшли ЗВО, що мають вищі за середні, але не кращі показники передумов ефективності участі в державних програмах розвитку освіти (мають вищу за медіанну інтегральну оцінки наявних переваг масштабів діяльності та спеціалізації), і високі показники якості підготовки (високі позиції в консолідованому рейтингу українських ЗВО).

Таке позиціювання свідчить про успішну реалізацію середнього і високого потенціалу: високі показники якості підготовки досягнуті за наявності близьких до середнього рівня передумовах ефективності участі в державних програмах розвитку освіти.

До третьої групи увійшли ЗВО, що обіймають високі позиції в рейтингу якості підготовки, маючі гірші медіанних передумови ефективності участі в державних програмах розвитку якості освіти (не мають переваг масштабу та спеціалізації порівняно з іншими ЗВО, проте забезпечують порівняно високу якість підготовки). Медіанне значення вектору інтегральних оцінок передумов ефективності участі в державних програмах розвитку освіти дорівнює 19,0, проте всі класифіковані

до третьої групи ЗВО мають інтегральну оцінку передумов ефективності участі в державних програмах менше 15-ти.

Нарешті всі інші ЗВО – четверта група. Ті, що за наявними даними не мають достатніх передумов для ефективності участі в державних програмах розвитку якості освіти та не демонструють високої позиції в рейтингах якості освіти.

В цій групі може бути виділена додаткова підгрупа: на рисунку 1 вони займають проміжне становище між другою і третьою групами ЗВО при цьому з мінімальним відставанням, як за показниками переваг масштабів і спеціалізації, так і за позицією в рейтингу якості підготовки.

Висновки і пропозиції щодо подальших досліджень

1. Досягнення певного (більшого за середній по дослідженим ЗВО) масштабу підготовки є недостатньою але необхідною умовою для високої очікуваної ефективності участі ЗВО в державних програмах розвитку освіти за 125-ою спеціальністю. Це дозволяє обґрунтувати як пріоритетність участі ЗВО з великими масштабами діяльності у державних програмах розвитку освіти за 125-ою спеціальністю, так і необхідність додаткового відбору учасників прогам державного сприяння розвитку освіти серед крупних ЗВО.

2. Перевага за ліцензованими обсягами не пов'язана з кращими результатами щодо якості підготовки, так само, як і гірші позиції за ліцензованими обсягами не виступають надійною ознакою гірших показників якості підготовки. Наведене узгоджується з результатами аналізу регіональної структури підготовки та дозволяє обґрунтувати тезу про вагому нерівномірність використання наявних у вітчизняних ЗВО передумов для розширення масштабів підготовки за 125-ою спеціальністю: наявний в одних ЗВО освітній потенціал реалізується не повною мірою, за одночасного надмірно інтенсивного навантаження (завеликих обсягах підготовки за 125-ою спеціальністю) виходячи з наявного кадрового та ресурсного потенціалу в інших ЗВО.

3. Переваги за концентрацією викладацьких кадрів, оцінені без урахування залучення викладачів до практичної діяльності щодо забезпечення кібербезпеки, опублікованих результатів наукової роботи, та успішного досвіду участі в міжнародних проєктах не пов'язані з перевагами за якістю підготовки для 125-ої спеціальності. Уточнення ролі викладацького потенціалу, кадрового забезпечення навчального процесу вимагає: по-перше, більш деталізованого оцінювання результатів викладачів, задіяних в підготовці за спеціальністю 125 «Кібербезпека»; по-друге, одержання оцінок якості підготовки у ЗВО бакалаврів та магістрів, що відображають її безпосередньо стосовно 125-ої спеціальності, а не опосередковано, через якість підготовки, властиву ЗВО загалом.

Література

[1] *Постанова від 29 квітня 2015 р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти»* [Електронний ресурс] – Режим доступу до ресурсу: https: //www.zakon.cc/law/document/read/266-2015-%D0%BF.

[2] *Про Стратегію кібербезпеки України: Указ Президента №96 / 2016* від 15.03.2016. URL: https:// zakon. rada.gov.ua/laws/show/96/2016.

[3] *Про основні засади забезпечення кібербезпеки України: Закон України* № № 2163-VIII від 05.10.2017 р. Відомості Верховної Ради (ВВР) [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov. ua/laws/show/2163-19#Text.

[4] ДСТУ ISO/IEC 27032:2016 (ISO/IEC27032: 2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки». 27.12.2016. № 448. [Електронний ресурс] – Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128.

[5] Доктрина інформаційної безпеки України [Електронний ресурс] – Режим доступу до ресурсу: // http://www.president.gov.ua/documents/472017-21374.

[6] Потій, О.В., Семенченко, А.І., Дубов, Д.В., Бакалинський, О.О., Мялковський, Д.В. Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України. ***Захист інформації***, Північна Америка, 23, кві. 2021. [Електронний ресурс] – Режим доступу до ресурсу: http://jrnl.nau.edu.ua/index. php/ZI/article/view/15434>.

[7] Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В. П. Шеломенцев // *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. — 2012. — Вип. 1. — С. 312-320.

[8] Діордіца І. В. *Поняття та зміст національної системи кібербезпеки* / І. В. Діордіца [Електронний ресурс]. — Режим доступу : http://goal-int.org/ponya ttyata-zmist-nacionalnoi-sistemi-kiberbezpeki/.

[9] Ліпкан В.А., Діордіца І. В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України */ Підприємництво, господарство і право*. Вип. 5, 2017 р. С. 174 – 180.

[10] Марущак А.І., Петров С.Г., Сучасний стан розвитку національної системи кібербезпеки (на прикладі СБ України та Держспецз'вязку України) / *Інформація і право. № 2(33)*, 2020. С. 77 – 84.

[11] Каленюк І.С., Куклін О.В. *Розвиток вищої освіти та економіка знань* / І.С Каленюк, Куклін О.В. – Київ: Знання, 2012. – 343 с.

[12] Бондар І. К., Сологуб О.П., Антошкіна Л.І., Бідак В.Я., Ільїч Л.М., Кичко І.І. *Інтелектуалізація людського капіталу: монографія* / І. К. Бондар (ред.). — К. : Корпорація, 2008. — 264 с.

[13] *Людський розвиток в Україні: можливості та напрями соціальних інвестицій (колективна науково-аналітична монографія)* / За ред. Е.М. Лібанової. – К.: Ін-т демографії та соціальних досліджень НАН України, Держкомстат України, 2006. – 355 с.

[14] Куклін О.В. *Стратегічні пріоритети розвитку вищої освіти України*// Вища освіта.- №8. - С.28-36.

[15] Грішнова О. А. *Освіта як чинник людського розвитку і економічного зростання України* [Електронний ресурс] / О. А. Грішнова. – Режим доступу : http://dspace.nbuv.gov.ua/bitstream/handle/123456789/1183/11-Grishnova.pdf?sequence=1.

[16] Бабич А. М., Егоров Е. В. *Экономика и финансирование социальной сферы*. — Центр Экспертизы и Маркетинга КТУ, 1996. — 512 с.

[17] *Human Development*. [Електронний ресурс] – Режим доступу до ресурсу: http://hdr.undp.org/en/data.

[18] *Міністерство освіти і науки України* [Електронний ресурс] – Режим доступу до ресурсу: https://mon.gov.ua/ua.

УДК 378:330;591.5

Potii O.V., Bakalynsky O.O., Myalkovsky D.V., Verba D.V. Resource provision and quality of cybersecurity specialists' training in the Ukrainian HEI as a prerequisite for participation in state programs of the educational specialty development

Abstract. *The article is devoted to a review of the preconditions that domestic High Education Institutions (HEI), where the specialty 125 "Cybersecurity" is licensed, have for quality training of the specialists, having appropriate qualifications, in connection with the characteristics of training quality (HEI position in the consolidated ranking of Ukrainian universities). Such preconditions include the scale of educational activities of the HEI, their specialization and compliance of the Department specialization with Passport of specialty 125 "Cybersecurity", the provision of the educational process by teachers with PhD and doctoral degrees. Aggregated, suitable for comparison assessment of resource potential of HEIs for high-quality training of cybersecurity specialists and indicators of such potential realization were calculated. According to the results the 56 HEIs, where cybersecurity specialists are trained, were divided into four groups. The first group includes HEIs, which occupy leading positions both in the presence of preconditions for quality training of cybersecurity professionals, and in assessing the quality of training. The second group includes HEIs that have higher than average, but not the best indicators of preconditions for quality training of cybersecurity professionals, and high indicators of training quality: such positioning indicates the successful implementation of medium and higher than medium potential. The third group includes HEIs who occupy high positions in the ranking of the quality of training, having the worse than median preconditions for quality training of cybersecurity professionals. Finally, the fourth group includes HEIs, which according to the available data do not have sufficient preconditions for high-quality training of cybersecurity specialists, which is confirmed by their positions in the consolidated ranking of Ukrainian universities.*

Keywords*: education, cybersecurity, staffing, higher education, quality of training.*

Потий А.В., Бакалинский А.О., Мялковский Д.В., Верба Д.В. Ресурсное обеспечение и качество подготовки специалистов по кибербезопасности в ВУЗах Украины как предпосылка участия в государственных программах содействия развитию образовательной специальности

Аннотация*. Статья посвящена обзору предпосылок, которые отечественные ВУЗы, лицензировавшие специальность 125 «Кибербезопасность», имеют для качественной подготовки специалистов соответствующей квалификации в связи с характеристикой качества подготовки (позицией ВУЗа в консолидированном рейтинге). К таким предпосылкам отнесены масштабы образовательной деятельности ВУЗа; его специализация и соответствие специализации кафедры набору компетенций, приобретаемых выпускниками специальности 125 «Кибербезопасность»; обеспеченность образовательного процесса преподавателями с кандидатской и докторской степенью. Определены агрегированные, пригодные для сравнения оценки ресурсного потенциала ВУЗов для качественной подготовки специалистов по кибербезопасности и показатели уровня использования такого потенциала. По результатам 56 ВУЗов, которые готовят специалистов по кибербезопасности разделены на четыре группы. К первой группе отнесены ВУЗы, занимающих ведущие позиции, как по наличию предпосылок качественной подготовки специалистов по кибербезопасности, так и по оценке качества подготовки. Во вторую группу вошли ВУЗы, с большими среднего и высокими показателями предпосылок качественной подготовки специалистов по кибербезопасности и высокими показателями качества подготовки (такое позиционирование свидетельствует об успешной реализации среднего и высокого потенциала). В третью группу вошли ВУЗы, занимающие высокие позиции в рейтинге качества подготовки, но имеющие худшие медианного значения показатели предпосылок качественной подготовки специалистов по кибербезопасности. Наконец, к четвертой группе отнесены ВУЗы, которые по имеющимся данным не имеют достаточных предпосылок для качественной подготовки специалистов по кибербезопасности, и занимающие низкие позиции в консолидированном рейтинге украинских вузов.*

Ключевые слова*: образование, кибербезопасность, кадровое обеспечение, высшее образование, качество подготовки.*

Потій Олександр Володимирович, д.т.н., професор, заступник Голови Державної служби спеціального зв'язку та захисту інформації України.

Потий Александр Владимирович, д.т.н., профессор, заместитель Председателя Государственной службы специальной связи и защиты информации Украины.
Oleksandr Potii, Doctor of Technical Sciences, Professor, Deputy Head of the State Service for Special Communications and Information Protection of Ukraine.

Бакалинський Олександр Олегович, к. т. н., заступник директора Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України.
Бакалинский Александр Олегович, к.т.н., Заместитель директора Департамента киберзащиты Администрации Государственной службы специальной связи и защиты информации Украины.
Bakalynsky Oleksandr, Candidate of Technical Sciences, Deputy Director of the Department of Cyber Defense of the Administration of the State Service for Special Communications and Information Protection of Ukraine.

Мялковський Данило Владиславович, к. д. у., директор Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язкутта захисту інформації України.
Мялковський Даниил Владиславович, кандидат наук по государственному управлению, директор Департамента киберзащиты Администрации Государственной службы специальной связи и защиты информации Украины.
Myalkovsky Danylo, Candidate of Sciences of Public Administration, Director of the Department of Cyber Defense of the Administration of the State Service for Special Communications and Information Protection of Ukraine.

Верба Денис Володимирович, к.е.н., доцент, доцент кафедри економічної теорії ДВНЗ «КНЕУ імені Вадима Гетьмана».
Верба Денис Владимирович, к.э.н., доцент, доцент кафедры экономической теории ГВУЗ «Киевский национальный экономический университет».
Verba Denys, Ph.D., Associate Professor department of Economic Theory, KNEU named after Vadym Hetman.

Отримано 20 *липня 2021 року*, затверджено редколегією *27 серпня 2021 року*

© Tarasenko Ya. The method of semantic noise addition according to the propagandist's individual semantic line // Ukrainian Scientific Journal of Information Security, 2021, vol. 27, issue 2, pp. 100-108. © ...

ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ / PRIVACY&PROTECTION FROM IDENTITY THEFT

DOI: 10.18372/2225-5036.27.16002

МЕТОД ДОДАВАННЯ СЕМАНТИЧНОГО ШУМУ ЗА ІНДИВІДУАЛЬНОЮ СЕМАНТИЧНОЮ ЛІНІЄЮ ПРОПАГАНДИСТА

Ярослав Тарасенко

Черкаський державний технологічний університет

ТАРАСЕНКО Ярослав Володимирович, к.т.н.

Рік та місце народження: 1993 рік, м. Черкаси, Україна.
Освіта: Черкаський державний технологічний університет, 2015 рік, Черкаський державний технологічний університет, 2017 рік.
Посада: старший викладач кафедри інформаційних технологій проектування, докторант кафедри інформаційної безпеки та комп'ютерної інженерії.
Наукові інтереси: комп'ютерна лінгвістична стеганографія, математична та прикладна лінгвістика, інформаційна безпека держави.
Публікації: більше 35 наукових публікацій (у тому числі статті, тези доповідей на конференціях, монографії).
E-mail: yaroslav.tarasenko93@gmail.com.
Orcid ID: 0000-0002-5902-8628.

Анотація. *Сучасні процеси в інформаційному полі держави зумовлюють зростання інтенсивності інформаційно-психологічного протиборства. Процеси здійснення зворотного впливу на зловмисника, який проводить деструктивну інформаційну пропаганду потребують вдосконалення з метою підвищення їх ефективності в протидії інформаційним загрозам держави та її громадян. Протиріччя, яке виникає при реалізації зворотного впливу на зловмисника, та полягає в тому, що цільовий текст повинен одночасно привертати увагу зловмисника та викривляти поле сприйняття структур, в яких приховані засоби зворотного впливу, може бути вирішено шляхом додавання семантичного інформаційного шуму за індивідуальною семантичною лінією пропагандиста. Однак існуючі підходи та методи, пов'язані з додаванням та опрацюванням інформаційного шуму в тексті не можуть бути використані для вирішення поставленої задачі, оскільки не враховують індивідуальну семантичну складову та допустимий інтервал ентропії семантичного шуму. Таким чином, було розроблено метод додавання семантичного шуму за індивідуальною семантичною лінією пропагандиста, що дозволяє зберегти неподільну семантичну складову, яка несе в собі основні засоби зворотного інформаційного впливу за умови привернення уваги зловмисника до тексту та підвищення загального рівня позитивного відношення до нього. Завдяки визначеному інтервалу оптимально допустимого доданого семантичного шуму, було описано модель формування англомовного тексту з доданим семантичним інформаційним шумом на основі вдосконаленого методу комп'ютеризованого формування англомовного тексту відповідно до психолінгвістичного портрету пропагандиста, що дозволило викривити світ сприйняття зловмисником неподільної семантичної складової для відволікання уваги пропагандиста від засобів зворотного впливу на нього та врівноваження конгруентної ситуації сприйняття семантичного шуму і неподільної семантичної складової.*

Ключові слова*: семантичний інформаційний шум, ентропія інформаційного шуму, негентропія, протидія пропаганді, психолінгвістичний портрет пропагандиста, інформаційно-психологічне протиборство, конгруентна ситуація.*

Вступ

Сучасні процеси в інформаційній сфері, державна політика та потенційні загрози інформаційній безпеці зумовлюють необхідність захисту прав та свобод громадян. Згідно Доктрини інформаційної безпеки України [1] до пріоритетів державної політики в інформаційній сфері, зокрема щодо забезпечення інформаційної безпеки відноситься недопущення використання інформаційного простору держави в деструктивних цілях та запобігання дій, що можуть призвести до дискредитації України на міжнародному рівні. Згаданий пріоритетний напрям передбачає протидію інформаційній пропаганді, шляхом зменшення рівня деструктивного впливу завдяки здійсненню зворотного інформаційного впливу на підсвідомість пропагандиста, що обґрунтовано в [2]. Також доводиться необхідність привернення уваги зловмисника до тексту з метою підвищення імовірності здійснення ефективного впливу. Однак, протиріччя полягає в тому, що для зменшення ефекту від застосування зловмисником методів протидії впливу на нього, зловмисник не повинен володіти інформацією про контейнер, де приховуються засоби зворотного впливу. Таким чином, додавання семантичного шуму в текст з метою відволікання уваги від неподільної семантичної складової [3], в якій приховується вплив є необхідною умовою для підвищення ефективності здійснення зворотного впливу на підсвідомість зловмисника, що зумовлює актуальність дослідження.

Аналіз досліджень та постановка завдання

Відповідно до [4], семантичний інформаційний шум допомагає виділити головне та приглушити другорядне, а, отже, цей інструмент можна використати для направлення зловмисника по хибному шляху, виділивши другорядне та приховавши головне, особливо, при врахуванні його психолінгвістичного портрету, процес матиме значно вищу ефективність.

Подібний підхід вперше розпочали вивчати американські лінгвісти, що спричинило появу ряду методів та теорій, на кшталт теорії конгруентності в сприйнятті повідомлення Озгуда і Таненбаума [5]. Відповідно, дослідження проводились на основі англійської мови, а, враховуючи найвищу розповсюдженість цієї мови в мережі Інтернет [6], використання згаданої теорії є доцільним.

При цьому, найбільш вдалим інструментом для впровадження інформаційного шуму в англомовний текст за допомогою комп'ютерних засобів є використання контекстуальної варіативності романських мов та асоціативних зв'язків, описаних в [7-8]. Розглянувши існуючі методи та засоби, що пов'язані з дослідженням чи додаванням інформаційного шуму [9-12], можна зробити висновок, що основна задача інформаційного шуму носить деструктивний характер, окрім окремих випадків, як збереження персональних даних, шляхом їх маскування. Проте, сучасні виклики процесам захисту інформації, змушують шукати підходи застосування нестандартних рішень та адаптацію їх до забезпечення інформаційної безпеки. Відповідно, базові підходи, що лежать в основі розглянутих методів, які пов'язані з інформаційним семантичним шумом, мають бути доопрацьовані відповідним чином. Враховуючи, що медіатекст є найкращим контейнером для впливу на громадян [13], а також властивості медіатексту, інформаційний шум поділяють на кількісний та якісний.

Кількісний в поставленій задачі володіє найвищою ентропією та легко видаляється, а тому слід розглядати лише якісний, який оснований на формі подачі відомостей [13]. Отже, в статті висувається гіпотеза про можливість використання семантичного інформаційного шуму для протидії інформаційному впливу на громадян, шляхом зміни базових підходів впровадження та функціонування якісного інформаційного шуму в рамках окремого тексту з метою здійснення зворотного інформаційного впливу на зловмисника із врахуванням його психолінгвістичного портрету. Отже, **метою роботи** є підвищення ефективності зворотного впливу на пропагандиста шляхом створення хибної неподільної семантичної складової на основі додавання семантичного інформаційного шуму та збереження справжньої неподільної семантичної складової, що несе в собі основні засоби зворотного інформаційного впливу на зловмисника.

В роботі ставляться наступні **задачі**:

1. Визначення інтервалу оптимально допустимого доданого семантичного шуму.
2. Опис моделі формування англомовного тексту з додаванням семантичного шуму за індивідуальною семантичною лінією пропагандиста на основі вдосконалення методу комп'ютеризованого формування англомовного тексту відповідно до психолінгвістичного портрету пропагандиста.
3. Формалізація процесу викривлення світу сприйняття зловмисником неподільної семантичної складової.

Методика дослідження

В основі процесу визначення оптимально допустимого доданого семантичного шуму покладено метод квантово-семантичного психолінгвістичного аналізу англомовного тексту пропагандного дискурсу [14], а теорія конгруентності [5] використовується для визначення допустимих меж доданого шуму при врівноваженні на позитивному значенні відношення

зловмисника до семантичного шуму та до засобів зворотного впливу на нього, прихованих в неподільній семантичній складовій. Модель формування англомовного тексту з доданим семантичним інформаційним шумом базується на використанні методу комп'ютеризованого формування англомовного тексту відповідно до психолінгвістичного портрету пропагандиста [15], що вдосконалено для можливості додавання семантичного шуму двох типів: синонімічного галуження, що проводиться на основі використання асоціативних зв'язків [7] чи впровадженні контекстуальної варіативності [8] та тематичної експлікації на основі методу виявлення і збереження неподільної семантичної складової англомовного маніпулятивного тексту пропагандного дискурсу [3]. Викривлення світу сприйняття зловмисником неподільної семантичної складової відбувається на основі методу квантово-семантичного психолінгвістичного аналізу англомовного тексту пропагандного дискурсу [14] з використанням семантики Монтегю та базуючись на методі виявлення і збереження неподільної семантичної складової англомовного маніпулятивного тексту пропагандного дискурсу [3]. Теорія конгруентності [5] дозволяє спрогнозувати ефект від проваджених дій.

Вирішення поставленої задачі

Згідно [16], інформаційний шум оснований на двох базових механізмах, ентропії та негентропії. В першому випадку, ентропією можна вважати рівень очікування появи тієї чи іншої семантичної конструкції, інакше кажучи, вона зумовлена зовнішніми факторами. Це впливає на сприйняття та інтерпретацію англомовного тексту пропагандистом. В свою чергу, негентропія є діаметрально протилежним механізмом, рівнем впорядкованості семантичної системи тексту, що характеризується хибним сприйняттям вже наявної в тексті інформації. Інакше кажучи, від цього механізму залежить рівень збереження неподільної семантичної складової англомовного тексту.

Визначення межі додавання семантичного шуму

За базовий підхід розрахунку ентропії можна взяти описаний в [14], оскільки метод квантово-семантичного психолінгвістичного аналізу англомовного тексту пропагандного дискурсу націлений на моделювання психолінгвістичного портрету пропагандиста та формування його психолінгвістичного профілю на основі ентропії. Таким чином, за [14] ентропія множини категорій семантичного ядра в контекстуальному зв'язку визначається як (1):

$$H(B_{n_r}^m) = \sum_{i=1}^{m} P(B_{n_r}^i) \cdot \log_2 \frac{1}{P(B_{n_r}^i)}, \qquad (1)$$

де $B_{n_r}^m$ – найнижчі категорії будь-якого ядра семантики; $P(B_{n_r}^m)$ – імовірність появи категорії ядра семантики. При цьому, на відміну від описаного методу розрахунку атрибуту психолінгвістичного впливу, необхідно враховувати особливості ентропії синонімічних конструкцій з ознаками психолінгвістичного впливу, які використовує зловмисник для уточнення загальної ентропії тексту.

Створений текст з доданими надлишковими шумовими структурами буде характеризуватись високою ентропією за рахунок додавання ентропії як окремих вказівників на ядро семантики, так і суми вказівників.

При цьому, важливим елементом виступає негентропія, що характеризує рівень впорядкованості неподільної семантичної складової, тобто ядра семантики, що не володіє надлишковістю, та яке неможливо видалити без втрати семантичної цілісності тексту.

Таким чином, загальна ентропія тексту з доданими до нього шумовими структурами, враховуючи психолінгвістичний портрет зловмисника та негентропію неподільної семантичної частки буде обраховуватись за формулою (2):

$$H(T_{exc}) = \sum_{i=1}^{m} P(B_{n_r}^i) \cdot \log_2 \frac{1}{P(B_{n_r}^i)} + H_{Q_n}(B_{n_r}^m) + \sum_{j=1}^{k} \sum_{i=1}^{m} P(O_{i,j}) \cdot \log_2 \frac{1}{P(O_{i,j})} - \sum_{i=1}^{m} P(B_L^i) \cdot \log_2 \frac{1}{P(B_L^{i_t})}, \qquad (2)$$

де T_{exc} – текст з доданими шумовими структурами; Q_n – синонімічні конструкції з ознаками психологічного впливу; $O_{m,k}$ – один з k вказівників на ядро семантики; $-\sum_{i=1}^{m} P(B_L^i) \cdot \log_2 \frac{1}{P(B_L^{i_t})}$ – негентропія ($H(B_L^{m_t})$), при тому, що $B_L^{m_t}$ – категоріальні значення реми/дирем тексту (становлять неподільну семантичну складову англомовного тексту пропагандного дискурсу), що основано на L рівні я-концепції зловмисника за часовою характеристикою тексту t.

Детально метод виявлення і збереження неподільної семантичної складової англомовного маніпулятивного тексту пропагандного дискурсу описано в [3].

Крім того, основуючись на обчисленні атрибуту психолінгвістичного впливу [14], значення $H_{Q_n}(B_{n_r}^m)$ обчислюється за формулою (3):

$$H_{Q_n}(B_{n_r}^m) = \sum_{i=1}^{n} \frac{\left|B_{i_r}^m\right|}{B_{i_r}^m} \cdot H(B_{i_r}^m) . \quad (3)$$

Однак, маючи зростаючу ентропію $H(T_{exc})$ слід виявити межу зростання, оскільки текст повинен залишитися осмисленим, при тому що повинна виконуватись задача зміщення фокусу зловмисника з неподільної семантичної складової.

В цьому випадку, відбувається зміна відношення зловмисника як до тексту в цілому, так і до його неподільної семантичної складової, а, отже, виникає протиріччя, або конгруентна ситуація. Для вирішення подібної ситуації слід скористатись теорією конгруентності [5].

Відповідно до теорії конгруентності, остаточний баланс буде досягнуто лише у випадку однакового відношення зловмисника до тексту та до неподільної семантичної складової, як по знаку, так і по інтенсивності. За знаком, відношення зловмисника до тексту позитивне (у зв'язку з додаванням семантичного шуму за психолінгвістичним портретом зловмисника), а до неподільної семантичної часки негативне (у зв'язку з приховуванням у ній маніпулятивних засобів, націлених на зловмисника).

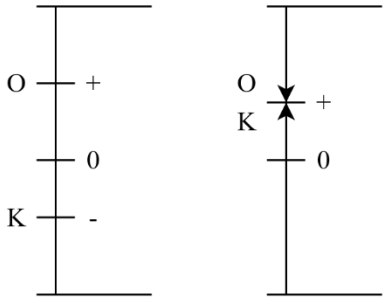
При цьому, на відміну від звичайної конгруентної ситуації, коли точка рівноваги допустима з від'ємним значенням, то в даному випадку, точка рівноваги має бути лише додатна, оскільки текст повинен справити позитивне враження на зловмисника та не викликати підозр, особливо в напрямку неподільної семантичної складової.

Таким чином, враховуючи, що зміна відношення $CtoT_{exc}$ зловмисника до тексту з доданими надлишковими шумовими структурами відбувається на основі процесу конгруентного врівноваження, то слід враховувати одночасно зміну відношення до надлишкових структур, що виражені загальною ентропією тексту з доданим семантичним шумом, так і відношення до неподільної семантичної складової, вираженої негентропією (4):

$$CtoT_{exc} = \begin{cases} CtoH(T_{exc}) = \dfrac{H(T_{exc})}{H(T_{exc}) + \left|H(B_L^{m_t})\right|} \cdot p' \\ CtoH(B_L^{m_t}) = \dfrac{\left|H(B_L^{m_t})\right|}{H(T_{exc}) + \left|H(B_L^{m_t})\right|} \cdot p' \end{cases}, \quad (4)$$

де $CtoH(T_{exc})$ – зміна відношення зловмисника до семантичного шуму; $CtoH(B_L^{m_t})$ – зміна відношення зловмисника до неподільної семантичної складової; p' – величина сумарної зміни відношень, що необхідно для досягнення рівноваги та розраховується за допомогою семантичного диференціалу. При цьому, значення $\left|H(B_L^{m_t})\right|$ береться по модулю, оскільки, негентропія є від'ємна та знаходиться на оціночній шкалі відношення зловмисника до даного об'єкту нижче нуля, що доводить негативне ставлення зловмисника до впроваджених у неподільну семантичну складову засобів впливу на нього.

Як можна побачити на узагальненому графіку відношення зловмисника до інформаційного шуму та впроваджених засобів впливу в неподільну семантичну складову (рис. 1), метою врівноваження є зміна відношення зловмисника до неподільної семантичної складової в сторону позитивного відношення до неї.



а) б)

Рис. 1. Узагальнений графік відношення зловмисника до інформаційного шуму (О) та впроваджених засобів впливу в неподільну семантичну складову (К): а) до впровадження інформаційного шуму в текст; б) після впровадження

Однак, щоб уникнути імовірних ситуацій, при яких інформаційний шум може спричинити погіршення загального ставлення до тексту до від'ємного рівня, або досягти значного відхилення від загального інформаційного фону, слід визначити межу додавання семантичного шуму. В такому випадку необхідне виконання умови (5):

$$\begin{cases} \left|H(B_L^{m_t})\right| < H(T_{exc}) \le \ln(H(B_L^{m_t}) + H(T_{exc})) \cdot H(B_L^{m_t}) \\ \ln(H(B_L^{m_t}) + H(T_{exc})) \cdot H(B_L^{m_t}) \le C_{pub} \end{cases}, \quad (5)$$

де C_{pub} – константа ентропії медіатексту публіцистичного стилю; максимальна ентропія $H_{\max} = (\ln(H(B_L^{m_t}) + H(T_{exc})) \cdot H(B_L^{m_t}) \le C_{pub})$.

Таким чином, для врівноваження відношення зловмисника до тексту, необхідно мати ентропію тексту не нижчою за негентропію по модулю та рівну або нижчу за ентропію медіатексту, враховуючи проміжок, на якому вона набуває найбільш врівноважених значень.

Рівень доданого семантичного шуму буде обчислюватись за формулою (6):

$$\sum_{j=1}^{k}\sum_{i=1}^{m} P(O_{i,j})\cdot\log_2\frac{1}{P(O_{i,j})} = H(T_{exc}) - \sum_{i=1}^{m} P(B_{n_r}^i)\cdot\log_2\frac{1}{P(B_{n_r}^i)} - H_{Q_n}(B_{n_r}^m) + \sum_{i=1}^{m} P(B_L^{i_t})\cdot\log_2\frac{1}{P(B_L^i)}, \quad (6)$$

при обов'язковому виконанні умови (5).

Формування англомовного тексту з додаванням семантичного шуму

Для отримання підґрунтя до фінального етапу методу – відволікання уваги зловмисника від неподільної семантичної складової, необхідно сформувати модель, за якою буде відбуватись додавання надлишкових семантичних шумових структур.

Щоб відношення до семантичного шуму було позитивним, що є обов'язковою умовою, наявність якої доведена вище, необхідно враховувати психолінгвістичні особливості зловмисника, за якими формувати вихідний англомовний текст.

Таким чином, згідно з [17] контекстуальна надлишковість показує, що обмеження, зумовлені порядком слів в англійській мові, семантико-синтаксичною структурою та лексичними значеннями оточуючих слів створюють умови, коли пропущене чи відсутнє слово являється надлишковим, або таким, що не додає нового у текст.

Це підтверджується взаємодією теми та реми у тексті, де тема є вже відомою інформацією, рема – новою, а збереження реми через її приховування зумовлює необхідність застосування теми, шляхом її уточнення чи синонімічної заміни об'єктів теми. Звідси слідує, що існує 2 типи моделей додавання семантичного шуму: за допомогою синонімічного галуження, що можливо впровадити через уточнення вже відомої теми завдяки асоціативним зв'язкам [7] та контекстуальній варіативності [8]; за допомогою експлікації теми базуючись на методі збереження неподільної семантичної складової [3].

Таким чином, модель додавання семантичного шуму за допомогою синонімічного галуження S буде описуватись формулою (7):

$$S_{exc} = \sum_{i=1}^{u}(B_{noun}^j + B_{verb}^j + B_{adj}^j)_i, \quad (7)$$

де $B_{noun}^j + B_{verb}^j + B_{adj}^j$ – найвищі категоріальні значення синонімічної конструкції відповідно іменника, дієслова та прикметника, в послідовній хронології пов'язаних з синонімічною групою теми, що разом складають групу вказівника (d') на ядро семантики, яке відповідає темі; u – потужність множини асоціативного поля зловмисника. Множину асоціативного поля пропагандиста можна виділити, застосувавши етап побудови типового психолінгвістичного профілю, описаний в [14]. При цьому $H(S_{exc}) \le H_{\max}$, а множина асоціативного поля зловмисника $U \in L^h$, де L^h – логічний рівень я-концепції особистості зловмисника. Детально визначення логічного рівня наводиться в [3]. Таким чином, можна отримати суму синонімічних вказівників на ядро семантики, які відрізняються лише морфологічно, але тотожні за структурою та семантичним значенням. Подібну модель можна порівняти з явищем плеоназму (дублювання семантичної складової в рамках граматичного структурного елементу). При цьому, враховується синонімічне галуження, як окремих лексичних компонентів так і граматичних структур в рамках асоціативного поля пропагандиста.

Формування тексту за моделлю додавання семантичного шуму можна описати формулою (8) при вдосконаленні методу [15]:

$$T = \prod_{i=0}^{d}\sum_{j=0}^{k} d_i'^j \cdot \prod_{i=0}^{d}\sum_{j=0}^{k}(d' \in U \mid G'^{b^j} > 0{,}5)_i, \quad (8)$$

де $\prod_{i=0}^{d}\sum_{j=0}^{k}(d' \in U \mid G'^{b^j} > 0{,}5)_i$ – синонімічні конструкції, які володіють відбитком психолінгвістичного портрету та належать до його асоціативного поля; G'^{b^k} – модифікований коефіцієнт Джині; d – кількість самостійних частин мови, що можуть бути використані в англомовному тексті, k – кількість синонімічних лексико-семантичних одиниць підкатегорії найнижчого порядку.

Друга модель реалізується за допомогою експлікації теми (9):

$$S'_{exc} = O_{0_n}^m - \sum_{k=1}^{m} O_{0_n}^k + \sum_{i=2}^{m} O_{0_n}^{i-1}, \quad (9)$$

де $O_{0_n}^m$ – множина початкових синонімічних об'єктів O_{0_n}, розподілених по m групах; $\sum_{k=1}^{m} O_{0_n}^k$ – головна тема тексту. При тому, $H(S'_{exc}) \le H_{\max}$, а, отже, формула зв'язного тексту матиме вигляд (10):

$$T_{exc} = \sum_{i=1}^{n} U^i + U^{i-1}, \quad (10)$$

де U – тема тексту. Таким чином, забезпечується, на ряду з класичною моделлю тексту, де тема послідовно змінюється з ремою, додавання семантичних складових, які уточнюють та доповнюють попередню тему, цим самим її розширюючи надлишковими елементами та поясненнями. Основуючись на наведеній моделі, можливо вдосконалити метод формування англомовного тексту з врахуванням індивідуальної семантичної лінії пропагандиста (11):

$$T_{exc} = \sum_{i=1}^{e} cd_{i-1}^{B^r} d_i^{B^r} \overline{S} + \sum_{i=2}^{e} cd_{i-1}^{B^r} \overline{S}\,, \qquad (11)$$

де c – коефіцієнт, який відповідає за відсоток збереження ядра семантики B^r, що характерне пропагандисту; d – група вказівника на ядро семантики; $\overline{S}$ – вектор синтаксичної одиниці з урахуванням характерних квантових станів сприйняття ядер семантики пропагандистом.

При цьому допускається, як окреме використання кожної моделі, так і комплексне при виконанні умови (12), при якій сума ентропій доданого семантичного шуму з використанням обох моделей не перевищує максимальної межі:

$$H(S_{exc}) + H(S'_{exc}) \le H_{\max}\,, \qquad (12)$$

Викривлення світу сприйняття зловмисником неподільної семантичної складової

Перш за все, з метою зміни сприйняття зловмисником неподільної семантичної складової, необхідно знайти ядро семантики неподільної семантичної складової за групою вказівника. В [3] описується процес пошуку групи вказівника (d'') на ядро семантики, що відповідає ремі. В такому випадку, маючи: групу вказівника, можна знайти ядро за формулою (13):

$$D'' = d'' / \left\{ B_n^m \mid z_n \in B_n^m \right\}, \qquad (13)$$

де B_n^m – найвище категоріальне значення; z_n – множина синонімів підтем.

Функція сюр'єктивного відображення ядра семантики (14) використовується в процесу зміни сприйняття зловмисником неподільної семантичної складової:

$$F_D : D'' \to \dot{D}\,, \qquad (14)$$

де $\dot{D}$ - ядро семантики, що не є ремою та частиною неподільної семантичної складової.

Це необхідно для зміщення уваги зловмисника з неподільної семантичної складової в напрямку семантичного ядра з семантичною надлишковістю, викликаною додаванням семантичного шуму, а, отже, для підвищення рівня позитивного відношення до тексту при вирішенні конгруентної ситуації.

Враховуючи особливості визначення світу сприйняття пропагандиста [14], можна обрахувати викривлений світ сприйняття $\dot{W}$ за формулою (15):

$$\dot{W} = \sum_{j=1}^{k}\sum_{i=1}^{m} P(O_{i,j}) \cdot \log_2 \frac{1}{P(O_{i,j})} \cdot \sum_{i=1}^{\left|S_2^*\right|} P(S_2^*) \cdot \log_2 \frac{1}{P(S_2^*)} \cdot \int F_D : \dot{D}_{<e,t>, S_2^*, W, Attr(Q_n)^{S_2^* \times W}} d'W \cdot W_n\,, \qquad (15)$$

де $\sum_{j=1}^{k}\sum_{i=1}^{m} P(O_{i,j}) \cdot \log_2 \frac{1}{P(O_{i,j})}$ – ентропія доданого інформаційного шуму; $\dot{D}_{<e,t>}$ – змінена предикативна константа, S_2^* – індивідні семантичні елементи, W – множина світів сприйняття; $Attr(Q_n)$ – атрибут інформаційно-психологічного протиборства (особливості визначення наводяться в [14]); d' – група вказівника на ядро семантики, яке відповідає темі.

Таким чином, можна визначити найбільш імовірні послідовності категорій ядер семантики за напрямком розвитку індивідуальної семантичної лінії при викривленому світі сприйняття (16):

$$P(B_{n_r}^m \cdot \dot{W} \mid B_{n_r}^1 \cdot W', ..., B_{n_r}^{m-1} \cdot \dot{W}) = \frac{P(B_{n_r}^1 \cdot \dot{W}, ..., B_{n_r}^{m-1} \cdot \dot{W})}{\prod_{i=1}^{m-1} P(B_{n_r}^i \cdot \dot{W} \mid B_{n_r}^1 \cdot \dot{W}, ..., B_{n_r}^{i-1} \cdot \dot{W})}\,, \qquad (16)$$

де $\dot{W}$ – викривлений світ сприйняття.

Довести ефективність методу, можна, використовуючи теорію конгруентності (17):

$$C\,to\,T_{exc} = \begin{cases} C\,to\,H(T_{exc}) = \dfrac{H(T_{exc})}{H(T_{exc}) + \left|H(O_{m,k})\right|} \cdot p' \\ C\,to\,H(O_{m,k}) = \dfrac{\left|H(O_{m,k})\right|}{H(T_{exc}) + \left|H(O_{m,k})\right|} \cdot p' \end{cases}, \qquad (17)$$

де в формулу (4) замість негентропії підставляється ентропія вказівника на ядро семантики, що зумовлено викривленням світу сприйняття, а оскільки, на відміну від від'ємного значення негентропії, ентропія вказівника додатна, то відношення до тексту зловмисником буде підвищено за умови відволікання його уваги від неподільної семантичної складової, що підвищує ефективність зворотного впливу.

Висновки

Таким чином, в роботі вирішено актуальну наукову задачу підвищення ефективності зворотного впливу на пропагандиста шляхом створення хибного неподільної семантичної складової на основі розробки методу додавання семантичного інформаційного шуму за індивідуальною семантичною лінією пропагандиста, що дозволяє зберегти істину неподільну семантичну складову, що несе в собі основні засоби зворотного інформаційного впливу на зловмисника за умови привернення уваги зловмисника до тексту та підвищення загального рівня позитивного відношення до нього.

Визначено інтервал оптимально допустимого доданого семантичного шуму шляхом розрахунку максимального об'єму доданої ентропії на основі методу квантово-семантичного психолівнгвістичного аналізу англомовного тексту пропагандного дискурсу за рахунок застосування теорії конгруентності, що дозволило формалізувати визначення допустимих меж доданого шуму з метою врівноваження на позитивному значенні відношення зловмисника до семантичного шуму та до засобів зворотного впливу, прихованих в неподільній семантичній складовій.

Вдосконалено метод комп'ютеризованого формування англомовного тексту відповідно до психолінгвістичного портрету пропагандиста на основі застосування асоціативної зв'язності та контекстуальної варіативності, базуючись на методі збереження неподільної семантичної складової, що дозволяє описати модель формування англомовного тексту з доданим семантичним інформаційним шумом.

Формалізовано процес викривлення світу сприйняття зловмисником неподільної семантичної складової на основі збереження реми тексту за рахунок застосування інформаційної ентропії тексту при обчисленні атрибуту інформаційно-психологічного протиборства шляхом використання інтенсіональної логіки та законів контекстуальної єдності ядра семантики та вказівника, що дозволило відволікти увагу зловмисника від засобів зворотного впливу на нього та підвищити рівень зацікавленості текстом загалом.

В ході дослідження підтверджена висунута гіпотеза про можливість використання семантичного інформаційного шуму для протидії інформаційному впливу на громадян, шляхом зміни базових підходів впровадження та функціонування якісного інформаційного шуму в рамках окремого тексту з метою здійснення зворотного інформаційного впливу на зловмисника із врахуванням його психолінгвістичного портрету. Подальшого дослідження потребує процес врахування групового психолінгвістичного портрету при доданні семантичного інформаційного шуму в англомовний текст для здійснення зворотного впливу на групу зловмисників за умов протидії груповій інформаційній пропаганді.

Результати дослідження можливо використовувати в процесі вбудовування стегоповідомлення при синтезі англомовного тексту з використанням квантово-семантичних методів, а також для підвищення рівня синхронізації з індивідуальною семантикою пропагандиста при квантово-семантичній модифікації існуючого англомовного тексту.

Література

[1] Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України"». [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/47/2017 #Text.

[2] Я. В. Тарасенко, «Використання принципів квантової лінгвістики в інформаційному протиборстві», *Безпека інформації*, Том 25, № 2, 2019 . - С. 96-103.

[3] Я. В. Тарасенко, «Метод виявлення і збереження неподільної семантичної складової англомовного маніпулятивного тексту пропагандного дискурсу на основі квантового формалізму», *Вісник Черкаського державного технологічного університету: технічні науки*, № 1, 2021. – С. 70-78.

[4] Нечепуренко М. Ю. Семантический шум как научная проблема // Известия ЮФУ. Технические науки. 2005. №9. URL: https://cyberleninka.ru/article/n/semanticheskiy-shum-kak-nauchnaya-problema.

[5] C.E. Osgood, P.H. Tannenbaum, «The principle of congruity in the prediction of attitude change», *Psychological Review*, № 62(1), 1955. - pp. 42–55.

[6] N. S. Kamaruddin, A. Kamsin, L. Y. Por, H. Rahman, «A Review of Text Watermarking: Theory, Methods, and Applications», *IEEE Access*, Vol. 6, 2018. -pp. 8011-8028.

[7] А. В. Красник, «Ассоциативные связи в структуре метеополя английского языка по данным свободного ассоциативного эксперимента», *Вопросы психолингвистики*, № 23, 2015. - С. 191-198.

[8] В. И. Агамджанова «Контекстуально обусловленная вариативность единиц языка» *: Сборник научных трудов, Рига: ЛГУ им. П.Стучки*, 1989. - 208 с.

[9] J. R. Pickett, «Semantic noise and the classroom», *ETC: A Review of General Semantics*, Vol. 45, № 3, 1988. - pp. 278-280.

[10] M. Rodriguez-Garcia, M. Batet, D. Sánchez, «Semantic Noise: Privacy-Protection of Nominal Microdata through Uncorrelated Noise Addition», *Proceedings of the 27th International Conference on Tools with Artificial Intelligence*, Vietri sul Mare, Italy, November 9-11, 2015. - pp. 1106-1113.

[11] O. Dušek, D. M. Howcroft, V. Rieser, «Semantic Noise Matters for Neural Natural Language Generation», *Proceedings of the 12th International Conference on Natural Language Generation*, Tokyo, Japan, October–November, 2019. - pp. 421-426.

[12] R. Gupta, R. N. Rao, «Towards Semantic Noise Cleansing of Categorical Data based on Semantic Infusion», *eprint arXiv:2002.02238v1*, 2020. [Електронний ресурс] – Режим доступу: https://arxiv.org/abs/2002. 02238.

[13] Е. Н. Басовская, «Информационный шум как воздействующий компонент медиатекста», *Вестник Челябинского государственного университета*, № 7 (336), 2014. - С. 6-11.

[14] Я. В. Тарасенко, «Метод квантово-семантичного психолінгвістичного аналізу англомовного тексту пропагандного дискурсу», *Сучасні інформаційні системи*, Том 3, № 4, 2019. - С 62-68.

[15] Я. В. Тарасенко, «Метод комп'ютеризованого формування англомовного тексту відповідно до психолінгвістичного портрету пропагандиста», *Захист інформації*, Том 22, № 2, 2020. - С. 66-73.

[16] И. Д. Бондарь, «Информационный шум: виды, механизмы формирования, опасности функционирования», *Научные труды Республиканского института высшей школы*, Вып. 16, 2017. - С. 35-43.

[17] В. И. Агамджанова, «Контекстуальная избыточность лексического значения слова на материале английского языка», Рига: Издательство «Зинатне», 1977, 123 с.

УДК 004.056

Тарасенко Я. В. Метод добавления семантического шума по индивидуальной семантической линии пропагандиста

Аннотация. *Современные процессы в информационном поле государства обусловливают рост интенсивности информационно-психологического противоборства. Процессы осуществления обратного влияния на злоумышленника, который проводит деструктивную информационную пропаганду нуждаются в совершенствовании с целью повышения их эффективности в противодействии информационным угрозам государству и его граждан. Противоречие, которое возникает при реализации обратного воздействия на злоумышленника, и заключается в том, что целевой текст должен одновременно привлекать внимание злоумышленника и искажать поле восприятия структур, в которых скрыты средства обратного влияния, может быть решено путем добавления семантического информационного шума по индивидуальной семантической линией пропагандиста. Однако существующие подходы и методы, связанные с добавлением и обработкой информационного шума в тексте, не могут быть использованы для решения поставленной задачи, поскольку не учитывают индивидуальную семантическую составляющую и допустимый интервал энтропии семантического шума. Таким образом, был разработан метод добавления семантического шума по индивидуальной семантической линией пропагандиста, что позволяет сохранить неделимую семантическую составляющую, которая несет в себе основные средства обратного информационного воздействия при привлечении внимания злоумышленника к тексту и повышении общего уровня положительного отношения к нему. Благодаря определенному интервалу оптимально допустимого добавленного семантического шума, было описано модель формирования англоязычного текста с добавленным семантическим информационным шумом на основе усовершенствованного метода компьютеризированного формирования англоязычного текста в соответствии с психолингвистическим портретом пропагандиста, что позволило исказить мир восприятия злоумышленником неделимой семантической составляющей для отвлечения внимания пропагандиста от средств обратного влияния на него и уравновешивания конгруэнтной ситуации восприятия семантического шума и неделимой семантической составляющей.*

Ключевые слова: *семантический информационный шум, энтропия информационного шума, негэнтропия, противодействие пропаганде, психолингвистические портрет пропагандиста, информационно-психологическое противоборство, конгруэнтная ситуация.*

Tarasenko Ya. The method of semantic noise addition according to the propagandist's individual semantic line

Abstract. *Modern processes in the state's information field cause an increase in the intensity of information and psychological warfare. The processes of the reverse influence on the malefactor, who conducts destructive information propaganda need to be improved in order to increase their effectiveness in counteracting information threats to the state and its citizens. The contradiction that arises in implementing the reverse influence on the malefactor, and is that the target text must simultaneously attract the malefactor's attention and distort the field of structures' perception in which the means of the reverse influence are hidden can be solved by adding semantic information noise according to the propagandist's individual semantic line. However, the existing approaches and methods related to the information noise processing and addition into the text cannot be used to solve the posed problem, because they do not take into account the individual semantic component and the allowable entropy interval of the semantic noise. Thus, the method of semantic noise addition according to the propagandist's individual semantic line is developed, which allows to preserve the indivisible semantic component, that carries the main means of the reverse influence, provided paying the malefactor's attention to the text and increasing the overall level of his positive attitude to the text. Due to the defined interval of optimally permissible added semantic noise, the model of English text formation with added semantic information noise based on the improved method of English text's computerized formation in accordance with the propagandist's psycholinguistic portrait was described, which allowed to distort the malefactor's world of perception the indivisible semantic component for distraction of the propagandist's attention from means of the reverse influence on him and balancing a congruent situation of perception the semantic noise and the indivisible semantic component.*

Keywords*: semantic information noise, entropy of information noise, negentropy, counter propaganda, propagandist's psycholinguistic portrait, information and psychological warfare, congruent situation.*

Тарасенко Ярослав Володимирович, к.т.н., старший викладач кафедри інформаційних технологій проектування, докторант кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету.
Тарасенко Ярослав Владимирович, к.т.н., старший преподаватель кафедры информационных технологий проектирования, докторант кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета.
Yaroslav Tarasenko, Candidate of Engineering Sciences, Senior Lecturer at the Department of Information Technologies of Designing, Doctoral Student at the Department of Information Security and Computer Engineering of Cherkassy State Technological University.

Отримано 17 *липня 2021 року,* затверджено редколегією *27 серпня 2021 року*