changed characteristics. It is shown that the reverse phenomenon – decoding of information – is possible too. A brief mathematical description of this biotechnical device functioning was given as well as corresponding algorithm. It was shown that the functions of NBS biosensor for encoding / decoding can be expressed in two forms that can be applied in practice: in tabular form and in analytical form as a function or several functions. Some parts of performed work were theoretical. As a result of performed works the possibilities of application of this technical device - biosensor for coding of information signals were substantiated. Thus, our obtained results can be used to encode and transmit information on relevant chemicals. The proposed work opens new opportunities for information security in information systems.

Key words: physical model, biosensor, information protection, coding, information system.

Ключко Олена Михайлівна, кандидат біологічних наук (біофізика), доцент кафедри електроніки, робототехніки і технологій моніторингу та Інтернету речей Національного авіаційного університету.
E-mail: kelenaXX@ukr.net.
Orcid ID: 0000-0003-4982-7490.
Ключко Елена Михайловна, кандидат биологических наук (биофизика), доцент кафедры электроники, робототехники и технологий мониторинга и интернета вещей Национального авиационного университета.
Klyuchko Olena, Candidate of Sciences (Biophysics), Associate Professor Department of Electronics, Robotics, Monitoring and IoT Technologies National Aviation University.

Шутко Володимир Миколайович, Професор, Доктор технічних наук, завідувач кафедри електроніки, робототехніки і технологій моніторингу та Інтернету речей Національного авіаційного університету.
E-mail: vnshutko@ukr.net.
Orcid ID: 0000-0002-9761-5583.
Шутко Владимир Николаевич, Професор, Доктор технических наук, заведующий кафедрой электроники, робототехники и технологий мониторинга и Интернета вещей Национального авиационного университета.
Shutko Vladimir, Professor, Doctor of Sciences (Engineering). Head of Department of Electronics, Robotics, Monitoring and IoT Technologies National Aviation University.

Морозова Ірина Володимирівна, кандидат технічних наук, доцент кафедри електроніки, робототехніки і технологій моніторингу та Інтернету речей Національного авіаційного університету.
E-mail: iramoro@ukr.net.
Orcid ID: 0000-0002-4238-4001.
Морозова Ирина Владимировна, кандидат технических наук, доцент кафедры электроники, робототехники и технологий мониторинга и интернета вещей Национального авиационного университета.
Morozova Irina, Candidate of Sciences (Engineering), Associate Professor of Department of Electronics, Robotics, Monitoring and IoT Technologies, National Aviation University.

Білецький Анатолій Якович, доктор технічних наук, професор, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, професор кафедри електроніки, робототехніки та технологій моніторингу та Інтернету речей Національного авіаційного університету.
E-mail: abelnau@ukr.net.
https://orcid.org/0000-0002-3798-8150.
Белецкий Анатолий Яковлевич, доктор технических наук, профессор, заслуженный деятель науки и техники Украины, лауреат Гос. премии Украины в области науки и техники, профессор кафедры электроники, робототехники и технологий мониторингу и Интернета вещей Национального авиационного университета.
Beletsky Anatoly, Doctor of Science, Professor, Honored Scientist of Ukraine, Laureate of the State Prize of Ukraine in Science and Technology, Department of Electronics, Robotics, Monitoring and IoT Technologies, Professor, National Aviation University.

DOI: 10.18372/2410-7840.23.15727
УДК 004.056.53(045)

ЕМУЛЯТОР ЗАГРОЗ ДЛЯ ВЕРИФІКАЦІЇ СИСТЕМ ВИЯВЛЕННЯ КІБЕРАТАК

Анна Корченко, Юрій Дрейс, Юрій Нагорний, Володимир Бичков

На сьогодні, одними із розповсюджених систем захисту інформації є системи виявлення кібератак та системи виявлення вторгнень, останні з яких становлять особливий практичний та науковий інтерес. Також, функціональність сучасних систем виявлення та блокування вторгнень у значній мірі залежить від їх можливостей щодо виявлення нових кібератак у режимі реального часу. Для виявлення відповідних атакуючих дій використовуються спеціальні методи, моделі, засоби, програмне забезпечення і комплексні технічні рішення для систем виявлення вторгнень, які можуть залишатись ефективними при появі нових або модифікованих кіберзагроз. Однак, як показує практика при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, відповідні засоби не завжди залишаються ефективними. Отже, розробка засобів верифікації та проведення експериментальних досліджень відповідних технічних рішень, засобів і програмного забезпечення виявлення кібератак, зловжи-

вань та аномалій в інформаційних системах для підтвердження адекватності їх роботи є актуальним науковим завданням. Є низка робіт, таких як кортежна модель формування атакуючих середовищ, низка методів для виявлення аномальних станів, методологія побудови системи виявлення вторгнень, а також структурна модель обчислювальної системи для створення засобів виявлення кібератак та її алгоритмічне і програмне забезпечення. Для її верифікації необхідний спеціалізований емулятор кіберзагроз, оскільки відомі не підтримують необхідні формати даних, що застосовуються у авторській розробці. Виходячи з цього, метою роботи є розробка емулятора для проведення експериментального дослідження для підтвердження достовірності отриманих теоретичних положень, практичних результатів та адекватності роботи програмного модуля розробленої системи виявлення кібератак, що дозволить удосконалити функціональні властивості сучасних систем виявлення вторгнень для режиму реального часу.

***Ключові слова**: атаки, кібератаки, аномалії, системи виявлення вторгнень, системи виявлення аномалій, системи виявлення атак, системи виявлення кібератак, виявлення аномалій в комп'ютерних мережах.*

ВСТУП

Інформаційні системи (ІС) та технології, відіграють на сьогодні ключову роль у процесі створення, накопичення, передавання та зберігання інформаційних ресурсів. На сьогодні, одними із розповсюджених систем захисту інформації є системи виявлення кібератак та системи виявлення вторгнень (СВВ), останні з яких становлять особливий практичний та науковий інтерес. Це означає, що СВВ є перспективним класом систем захисту інформації, удосконалення та розвиток яких є пріоритетним напрямом наукових досліджень багатьох вчених.

Також, функціональність сучасних систем виявлення та блокування вторгнень у значній мірі залежить від їх можливостей щодо виявлення нових кібератак у режимі реального часу. Засоби систем протидії достатньо розвинуті, але для їх ефективної роботи необхідна відповідна інформація, за допомогою якої можливо виявляти атакуючі дії. Формування таких даних, як правило, здійснюється постфактум і потребує певного часу.

Постійна реалізація кібератак на різні державні та приватні критичні інформаційні інфраструктури потребує впровадження спеціальних технічних рішень та систем протидії.

Для виявлення відповідних атакуючих дій використовуються спеціальні методи [1-3], моделі [4-5], засоби [4, 6-7], програмне забезпечення (ПЗ) [4, 8-9] і комплексні технічні рішення для СВВ [4, 6, 9-10], які можуть залишатись ефективними при появі нових або модифікованих кіберзагроз.

Однак, як показує практика при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, відповідні засоби не завжди залишаються ефективними.

Отже, розробка засобів верифікації та проведення експериментальних досліджень відповідних технічних рішень, засобів і ПЗ виявлення кібератак, зловживань та аномалій в ІС для підтвердження адекватності їх роботи є актуальним науковим завданням.

В роботі [11, 12] розроблено кортежну модель формування атакуючих середовищ для відображення процесу виявлення аномального стану за заданий часовий проміжок в *m*-вимірному гетерогенному параметричному середовищі. У [13-17] запропоновано низку методів формування еталонів для формалізації процесу отримання еталонних середовищ, що містять множини значень фіксованих параметрів визначених груп лінгвістичних змінних. У дослідженнях [18] розроблені метод фазифікації на еталонних підсередовищах для перетворення поточних значень параметрів та дефазифікації параметрів детекційного середовища, для отримання числових оцінок, що характеризують лінгвістичні величини відносно суджень експерта. Також, у [19] запропоновано метод номіналізації нечітких чисел для визначення ідентифікуючих термів, що відображають стан поточних середовищ, характерних для реалізації визначених типів кібератак. А в [20] розроблено метод визначення ідентифікуючих термів, для пошуку в заданих лінгвістичних змінних перетворених еталонних термів, що характеризують певні рівні аномальності.

В роботі [21] запропоновано метод формування детекційного середовища для визначення поточних рівнів аномальних станів, характерних дії визначених типів кібератак. Базуючись на [11-

21] розроблено методологію побудови систем виявлення аномалій [22], породжених кібератаками для розширення функціональних можливостей сучасних СВВ. В роботі [23-25] на підставі [22] запропоновано структурну модель обчислювальної системи для створення засобів виявлення кібератак, а також її алгоритмічне та програмне забезпечення. Для її верифікації необхідний спеціалізований симулятор кіберзагроз, оскільки відомі [26-28] не підтримують необхідні формати даних, що застосовуються у авторській розробці [23].

Виходячи з цього, метою роботи є розробка емулятора для проведення експериментального дослідження для підтвердження достовірності отриманих теоретичних положень, практичних результатів та адекватності роботи програмного модуля розробленої системи виявлення кібератак (СВК) [23], що дозволить удосконалити функціональні властивості сучасних СВВ для режиму реального часу.

ОСНОВНА ЧАСТИНА

Відповідно до запропонованого структурного рішення СВК [23], яке базується на методології побудови систем виявлення аномалій, породжених кібератаками (МПСВ) [22] та з урахуванням [24, 29, 30], здійснимо верифікацію програмної моделі СВК [24, 29] з метою підтвердження достовірності теоретичних положень наукових досліджень, проведених у роботі.

Для цього розробимо структуру віртуальної мережі (рис. 1), за допомогою якої проведемо моделювання різних типів загроз РІС.

Така мережа складається з файл-сервера (ФС) (192.245.23.1), СВК і шести клієнтів (К) – К1 (192.245.23.2), К2 (192.245.23.3), К3 (192.245.23.4), К4 (192.245.23.5), К5 (192.245.23.6) та К6 (192.245.23.7).

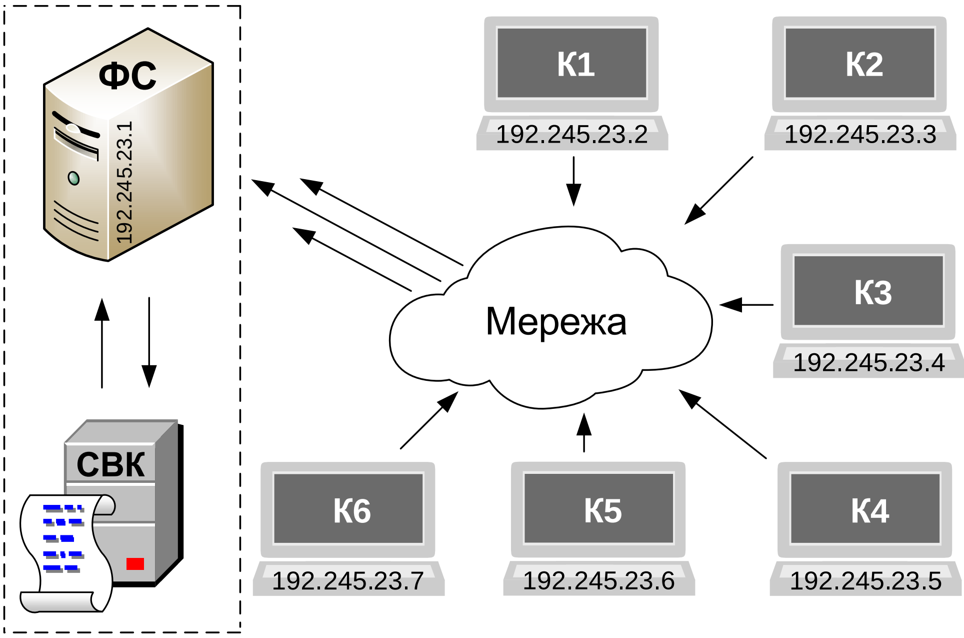

Рис. 1. Структура віртуальної мережі для моделювання атак

Для реалізації атак за допомогою віртуальної мережі розроблено клієнт серверний застосунок, що емулює роботу системи в режимі реального часу. Так, у вікні на рис. 2 відображено приклад приймання запитів від клієнтів і перевірка значення параметру «Кількість пакетів з однаковою адресою відправника та одержувача» (КПОА), а в момент підключення (відключення) нового клієнта здійснюється процес отримання значення параметру «Кількість одночасних підключень до сервера» (КОП) (інтервал між запитами складає 50 мс.). Для прикладу, сформуємо значення величин $\underset{\sim}{P}_{SPКОП}^{\tau_f}$ та $\underset{\sim}{P}_{SPКПОА}^{\tau_f}$ (spoofing (SP)) [25] поточного підсередовища ($\mathbf{P}_{\mathbf{i}}^{\tau_f} = \mathbf{P}_{\mathbf{3}}^{\tau_f}$) атакуючого середовища ($\mathbf{CA}^{\tau_f}$), які несуть мінімальну загрозу для ФС:

$$\underset{\sim}{P}_{SPКОП}^{\tau_f} = \{0/0{,}030;\ 0{,}4/0{,}030;\ 1/0{,}05;\ 0{,}2/0{,}07;\ 0/0{,}07\};$$

$$\underset{\sim}{P}_{SPКПОА}^{\tau_f} = \{0/0{,}030;\ 0{,}5/0{,}030;\ 1/0{,}05;\ 0{,}7/0{,}150;\ 0/0{,}150\}.$$

Далі, відповідно до номіналізованих нечітких чисел (НЧ) еталонного підсередовища($\mathbf{T_i^e} = \mathbf{T_3^e} = \mathbf{T_{SP}^e}$), визначених в [19, 25], здійснимо формування номіналізованого НЧ поточного підсередовища ($\mathbf{P_i^{\tau_f}} = \mathbf{P_3^{\tau_f}}$) з урахуванням [19], тобто:

$$\underset{\sim}{P}_{31}^{\tau_f p} = \{\bigcup_{g=1}^{13} \mu_{31g}^p / x_{31g}^p\} = \{\mu_{311}^p / x_{311}^p,\ \mu_{312}^p / x_{312}^p,$$
$$\mu_{313}^p / x_{313}^p,\ \mu_{314}^p / x_{314}^p,\ \mu_{315}^p / x_{315}^p,\ \mu_{316}^p / x_{316}^p,$$
$$\mu_{317}^p / x_{317}^p,\ \mu_{318}^p / x_{318}^p,\ \mu_{319}^p / x_{319}^p,\ \mu_{31(10)}^p / x_{31(10)}^p,$$
$$\mu_{31(11)}^p / x_{31(11)}^p,\ \mu_{31(12)}^p / x_{31(12)}^p,\ \mu_{31(13)}^p / x_{31(13)}^p\},$$

де: $\mu_{311}^p = \mu_{31(13)}^p = AL_{311} = 0,$

$$\mu_{312}^p = \mu_{31(12)}^p = AL_{312} = 0{,}2,\ \mu_{313}^p = \mu_{31(11)}^p = AL_{313} = 0{,}3,$$
$$\mu_{314}^p = \mu_{31(10)}^p = AL_{314} = 0{,}4,\ \mu_{315}^p = \mu_{319}^p = AL_{315} = 0{,}6,$$
$$\mu_{316}^p = \mu_{318}^p = AL_{316} = 0{,}7,\ \mu_{317}^p = \mu_{317}^p = AL_{317} = 1,$$
$$\mu_{311}^p = \mu_{311} = 0,\ x_{311}^p = x_{311} = 0{,}030 \text{ та}$$

$$\underset{\sim}{P}_{32}^{\tau_f p} = \{\bigcup_{g=1}^{9} \mu_{32g}^p / x_{32g}^p\} = \{\mu_{321}^p / x_{321}^p,\ \mu_{322}^p / x_{322}^p,$$
$$\mu_{323}^p / x_{323}^p,\ \mu_{324}^p / x_{324}^p,\ \mu_{325}^p / x_{325}^p,\ \mu_{326}^p / x_{326}^p,$$
$$\mu_{327}^p / x_{327}^p,\ \mu_{328}^p / x_{328}^p,\ \mu_{329}^p / x_{329}^p\},$$

де: $\mu_{321}^p = \mu_{329}^p = AL_{321} = 0,\ \mu_{322}^p = \mu_{328}^p = AL_{322} = 0{,}2,\ \mu_{323}^p = \mu_{327}^p = AL_{323} = 0{,}5,\ \mu_{324}^p = \mu_{326}^p = AL_{324} = 0{,}7,\ \mu_{325}^p = \mu_{325}^p = AL_{325} = 1,\ \mu_{321}^p = \mu_{321} = 0,\ x_{321}^p = x_{321} = 0{,}030.$

Далі, формування номіналізованого НЧ $\underset{\sim}{P}_{ij}^{\tau_f p} = \underset{\sim}{P}_{31}^{\tau_f p}$ поточного підсередовища ($\mathbf{P_i^{\tau_f}} = \mathbf{P_3^{\tau_f}}$) здійснюється за допомогою α-рівневих інтервалів $\mathbf{AL_{31}^{Ip}}$ [19, 25] при $\rho = 5$, а

$$\mu_{31max} = \bigvee_{q=1}^{\rho} \mu_{31q} = \mu_{311} \vee \mu_{312} \vee \mu_{313} \vee \mu_{314} \vee \mu_{315} =$$
$$0 \vee 0{,}4 \vee 1 \vee 0{,}2 \vee 0 = \mu_{313} = 1$$

та якщо:

- $r_1 = 1,\ c = \overline{1,k_1},\ k_1 = 3$ і

$$(\mu_{311} < AL_{311c}^{Ip} \le \mu_{312}) \wedge (x_{312} \le x_{31max})$$
$$((0 < AL_{311c}^{Ip} \le 0{,}4) \wedge (0{,}030 \le 0{,}05)), \text{ то}$$

$$\mathbf{AL_{311}^{Ip}} = \{\bigcup_{c=1}^{k_1} AL_{311c}^{Ip}\} = \{AL_{3111}^{Ip},\ AL_{3112}^{Ip},$$
$$AL_{3113}^{Ip}\} = \{0{,}2;\ 0{,}3;\ 0{,}4\};$$

- $r_2 = 2,\ c = \overline{1,k_2},\ k_2 = 3,$

$$(\mu_{312} < AL_{312c}^{Ip} \le \mu_{313}) \wedge (x_{313} \le x_{31max})$$
$$((0{,}4 < AL_{312c}^{Ip} \le 1) \wedge (0{,}05 \le 0{,}05)), \text{ то}$$

$$\mathbf{AL_{312}^{Ip}} = \{\bigcup_{c=1}^{k_2} AL_{312c}^{Ip}\} = \{AL_{3121}^{Ip},\ AL_{3122}^{Ip},$$
$$AL_{3123}^{Ip}\} = \{0{,}6;\ 0{,}7;\ 1\};$$

- $r_3 = 3,\ c = \overline{1,k_3},\ k_3 = 5,$

$$(\mu_{313} > AL_{313c}^{Ip} \ge \mu_{314}) \wedge (x_{314} \ge x_{31max})$$
$$((1 > AL_{313c}^{Ip} \ge 0{,}2) \wedge (0{,}07 \ge 0{,}05)), \text{ то}$$

$$\mathbf{AL_{313}^{Ip}} = \{\bigcup_{c=1}^{k_3} AL_{313c}^{Ip}\} = \{AL_{3131}^{Ip},\ AL_{3132}^{Ip},\ AL_{3133}^{Ip},$$
$$AL_{3134}^{Ip},\ AL_{3135}^{Ip}\} =$$
$$\{0{,}7;\ 0{,}6;\ 0{,}4;\ 0{,}3;\ 0{,}2\};$$

- $r_4 = 4,\ c = \overline{1,k_4},\ k_4 = 1,$

$$(\mu_{314} > AL_{314c}^{Ip} \ge \mu_{315}) \wedge (x_{315} \ge x_{31max})$$
$$((0{,}2 > AL_{314c}^{Ip} \ge 1) \wedge (0{,}07 \ge 0{,}05)), \text{ то}$$

$$\mathbf{AL_{314}^{Ip}} = \{\bigcup_{c=1}^{k_4} AL_{314c}^{Ip}\} = \{AL_{3141}^{Ip}\} = \{0\}.$$

З урахуванням обчислених значень, отримаємо наступний вигляд:

$$\mathbf{AL_{31}^{Ip}} = \{\bigcup_{b=1}^{\rho-1}\{\bigcup_{c=1}^{k_b} AL_{31bc}^{Ip}\}\} = \{\{AL_{3111}^{Ip},\ AL_{3112}^{Ip},$$
$$AL_{3113}^{Ip}\},\ \{AL_{3121}^{Ip},\ AL_{3122}^{Ip},\ AL_{3123}^{Ip}\},$$
$$\{AL_{3131}^{Ip},\ AL_{3132}^{Ip},\ AL_{3133}^{Ip},\ AL_{3134}^{Ip},\ AL_{3135}^{Ip}\},$$
$$\{AL_{3141}^{Ip}\}\} = \{\{0{,}2;\ 0{,}3;\ 0{,}4\},\ \{0{,}6;\ 0{,}7;\ 1\},\ \{0{,}7;\ 0{,}6;$$
$$0{,}4;\ 0{,}3;\ 0{,}2\},\ \{0\}\}.$$

За аналогією з прикладом, для $\underset{\sim}{P}_{31}^{\tau_f p}$ формування номіналізованого НЧ $\underset{\sim}{P}_{ij}^{\tau_f p} = \underset{\sim}{P}_{32}^{\tau_f p}$ поточного підсередовища ($\mathbf{P_i^{\tau_f}} = \mathbf{P_3^{\tau_f}}$) реалізується на основі [19, 25] за допомогою α-рівневих інтервалів $\mathbf{AL_{32}^{Ip}}$, тобто:

$$\mathbf{AL_{32}^{Ip}} = \{\bigcup_{b=1}^{\rho-1}\{\bigcup_{c=1}^{k_b} AL_{32bc}^{Ip}\}\} = \{\{AL_{3211}^{Ip},\ AL_{3212}^{Ip}\},$$
$$\{AL_{3221}^{Ip},\ AL_{3222}^{Ip}\},\ \{AL_{3231}^{Ip}\},\ \{AL_{3241}^{Ip},\ AL_{3242}^{Ip},\ AL_{3243}^{Ip},$$
$$AL_{3244}^{Ip}\}\} = \{\{0{,}2;\ 0{,}5\},\ \{0{,}7;\ 1\},\ \{0{,}7\},\ \{0{,}5;$$
$$0{,}2;1\}\}.$$

Обчислення значень x_{31g}^p для перетворених НЧ $\underset{\sim}{P}_{31}^{\tau_f p} = \underset{\sim}{P}_{SPKOП}^{\tau_f p}$ поточного підсередовища ($\mathbf{P_i^{\tau_f}} = \mathbf{P_3^{\tau_f}}$) здійснюється аналогічно до кроку 4 в [19] з урахуванням [19, 25] при $z = 13,\ g = \overline{2,13}$ на основі компонентів μ_{ijg} / x_{ijg}, тобто $\mu_{311}=0$, $\mu_{312}=0{,}4$, $x_{311}=0{,}03$ та $x_{312}=0{,}03$.

Далі, з урахуванням цього:

- якщо $\mu^{p}_{312}=AL^{lp}_{312}=0{,}2$, то

$x^{p}_{312}=0{,}03+((0{,}2-0)\cdot(0{,}03-0{,}03))/(0{,}4-0)=0{,}03$;

- якщо $\mu^{p}_{313}=AL^{lp}_{313}=0{,}3$, то

$x^{p}_{313}=0{,}03+((0{,}3-0)\cdot(0{,}03-0{,}03))/(0{,}4-0)=0{,}03$;

- якщо $\mu^{p}_{314}=AL^{lp}_{314}=0{,}4$, то

$x^{p}_{314}=0{,}03+((0{,}4-0)\cdot(0{,}03-0{,}03))/(0{,}4-0)=0{,}03$.

Наступним, при $\mu_{312}=0{,}4$, $\mu_{313}=1$, $x_{312}=0{,}03$ та $x_{313}=0{,}05$:

- якщо $\mu^{p}_{315}=AL^{lp}_{315}=0{,}6$, то

$x^{p}_{315}=0{,}03+((0{,}6-0{,}4)\cdot(0{,}05-0{,}03))/(1-0{,}4)=0{,}037$;

- якщо $\mu^{p}_{316}=AL^{lp}_{316}=0{,}7$, то

$x^{p}_{316}=0{,}03+((0{,}7-0{,}4)\cdot(0{,}05-0{,}03))/(1-0{,}4)=0{,}04$;

- якщо $\mu^{p}_{317}=AL^{lp}_{317}=1$, то

$x^{p}_{317}=0{,}03+((1-0{,}4)\cdot(0{,}05-0{,}03))/(1-0{,}4)=0{,}05$.

Далі, при $\mu_{313}=1$, $\mu_{314}=0{,}2$, $x_{313}=0{,}05$ та $x_{314}=0{,}07$ обчислимо:

- якщо $\mu^{p}_{318}=AL^{lp}_{318}=0{,}7$, то

$x^{p}_{318}=0{,}03+((0{,}7-1)\cdot(0{,}07-0{,}05))/(0{,}2-1)=0{,}038$;

- якщо $\mu^{p}_{319}=AL^{lp}_{319}=0{,}6$, то

$x^{p}_{319}=0{,}03+((0{,}6-1)\cdot(0{,}07-0{,}05))/(0{,}2-1)=0{,}04$;

- якщо $\mu^{p}_{31(10)}=AL^{lp}_{31(10)}=0{,}4$, то

$x^{p}_{31(10)}=0{,}03+((0{,}4-1)\cdot(0{,}07-0{,}05))/(0{,}2-1)=0{,}045$;

- якщо $\mu^{p}_{31(11)}=AL^{lp}_{31(11)}=0{,}3$, то

$x^{p}_{31(11)}=0{,}03+((0{,}3-1)\cdot(0{,}07-0{,}05))/(0{,}2-1)=0{,}048$;

- якщо $\mu^{p}_{31(12)}=AL^{lp}_{31(12)}=0{,}2$, то

$x^{p}_{31(12)}=0{,}03+((0{,}2-1)\cdot(0{,}07-0{,}05))/(0{,}2-1)=0{,}05$.

Наступним, при $\mu_{314}=0{,}2$, $\mu_{315}=0$, $x_{314}=0{,}07$ та $x_{315}=0{,}07$ для $\mu^{ep}_{31(13)}=AL^{lp}_{31(13)}=0$ визначимо $x^{ep}_{31(13)}=0{,}07+((0-0{,}2)\cdot(0{,}07-0{,}07))/(0-0{,}2)=0{,}07$, а $\mu^{p}_{311}=\mu_{311}=0$, $x^{p}_{311}=x_{311}=0{,}03$.

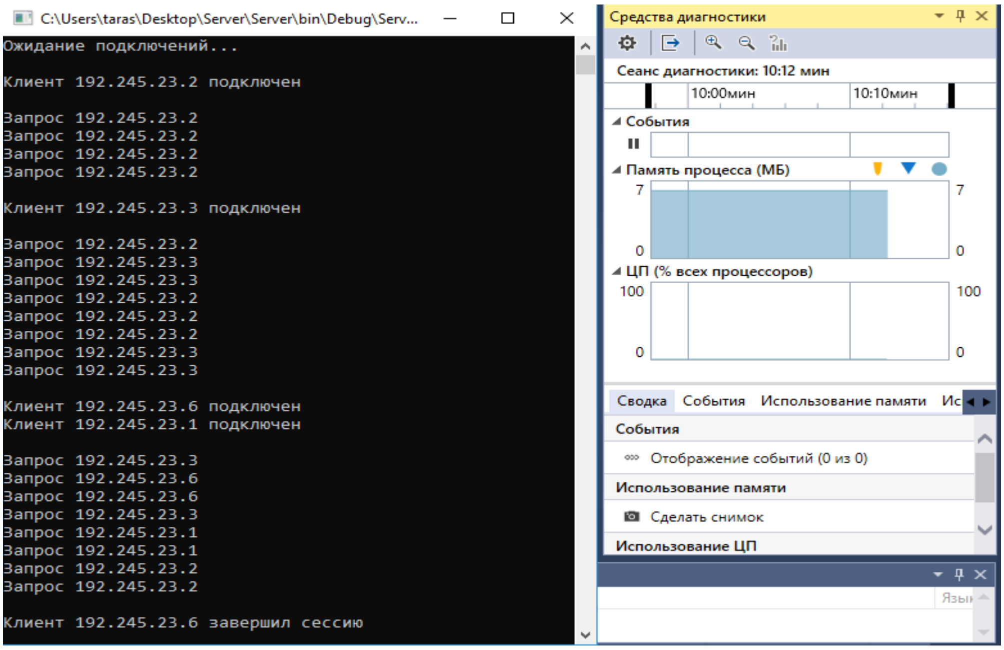

Рис. 2. Відображення процесів, пов'язаних із функціонуванням ФС у віртуальній мережі

Таким чином, номіналізоване НЧ поточного підсередовища ($\mathbf{P}^{\tau_f}_{\mathbf{i}}=\mathbf{P}^{\tau_f}_{\mathbf{3}}$) відповідно до [19] прийме наступний вигляд:

$$\underset{\sim}{P}^{\tau_f p}_{31}=\underset{\sim}{P}^{\tau_f p}_{SPKOП}=\{0/0{,}03;\ 0{,}2/0{,}03;\ 0{,}3/0{,}03;\ 0{,}4/0{,}03;\ 0{,}6/0{,}037;\ 0{,}7/0{,}04;\ 1/0{,}05;\ 0{,}7/0{,}038;\ 0{,}6/0{,}04;\ 0{,}4/0{,}045;\ 0{,}3/0{,}048;\ 0{,}2/0{,}05;\ 0/0{,}07\}.$$

Обчислення значень x^{p}_{36g} для перетворених НЧ $\underset{\sim}{P}^{\tau_f p}_{32}=\underset{\sim}{P}^{\tau_f p}_{SPKПОД}$ поточного підсередовища ($\mathbf{P}^{\tau_f}_{\mathbf{i}}=\mathbf{P}^{\tau_f}_{\mathbf{3}}=\mathbf{P}^{\tau_f}_{\mathbf{SP}}$) здійснюється аналогічно, з урахуванням [19] при $z=9$, за допомогою компонентів μ_{ijg} / x_{ijg}, тобто при $\mu_{321}=0$, $\mu_{322}=0{,}5$, $x_{321}=0{,}03$ та $x_{322}=0{,}03$.

Далі, з урахуванням цих значень:

- якщо $\mu^{p}_{322}=AL^{lp}_{322}=0{,}2$, то $x^{p}_{322}=0{,}03$;
- якщо $\mu^{p}_{323}=AL^{lp}_{323}=0{,}5$, то $x^{p}_{323}=0{,}03$.

При $\mu_{322}=0{,}5$, $\mu_{323}=1$, $x_{322}=0{,}03$ та $x_{323}=0{,}05$:

- якщо $\mu^{p}_{324}=AL^{lp}_{324}=0{,}7$, то $x^{p}_{324}=0{,}038$;

- якщо $\mu_{325}^{p} = AL_{325}^{Ip} = 1$, то $x_{325}^{p} = 0{,}05$.

Далі, при $\mu_{323} = 1$, $\mu_{324} = 0{,}7$, $x_{323} = 0{,}05$ та $x_{324} = 0{,}15$ для $\mu_{326}^{p} = AL_{326}^{Ip} = 0{,}7$ обчислимо $x_{326}^{p} = 0{,}15$.

І, нарешті, при $\mu_{324} = 0{,}7$, $\mu_{325} = 0$, $x_{324} = 0{,}15$ та $x_{325} = 0{,}15$ для $\mu_{327}^{p} = AL_{327}^{Ip} = 0{,}5$, $\mu_{328}^{p} = AL_{328}^{Ip} = 0{,}2$, $\mu_{329}^{p} = AL_{329}^{Ip} = 0$ відповідно обчислимо $x_{327}^{p} = x_{328}^{p} = x_{329}^{p} = 0{,}15$, а $\mu_{321}^{p} = \mu_{321} = 0$, $x_{321}^{p} = x_{321} = 0{,}03$.

Таким чином, номіналізоване НЧ поточного підсередовища ($\mathbf{P_i^{\tau_f}} = \mathbf{P_3^{\tau_f}} = \mathbf{P_{SP}^{\tau_f}}$) відповідно до [19] має вигляд:,

$$\underset{\sim}{P}_{32}^{\tau_f p} = \underset{\sim}{P}_{SPKПОА}^{\tau_f p} = \{0/0{,}03;\ 0{,}2/0{,}03;\ 0{,}5/0{,}03;\ 0{,}7/0{,}378;\ 1/0{,}05;\ 0{,}7/0{,}15;\ 0{,}5/0{,}15;\ 0{,}2/0{,}15;\ 0/0{,}15\}.$$

Зведемо отримані дані до узагальнювальних табл. 1-2.

Таблиця 1

Узагальнювальна таблиця для $\underset{\sim}{P}_{SPKОП}^{p}$

$\underset{\sim}{P}_{31}^{\tau_f p}$	$\mu_{31g}^{p}\ (g=\overline{1,13})$												
	μ_{311}^{p}	μ_{312}^{p}	μ_{313}^{p}	μ_{314}^{p}	μ_{315}^{p}	μ_{316}^{p}	μ_{317}^{p}	μ_{318}^{p}	μ_{319}^{p}	$\mu_{31(10)}^{p}$	$\mu_{31(11)}^{p}$	$\mu_{31(12)}^{p}$	$\mu_{31(13)}^{p}$
	0	0,2	0,3	0,4	0,6	0,7	1	0,7	0,6	0,4	0,3	0,2	0
$\underset{\sim}{P}_{SPKОП}^{\tau_f p}$	0,03	0,03	0,03	0,03	0,037	0,04	0,05	0,038	0,04	0,045	0,048	0,05	0,07

Таблиця 2

Узагальнювальна таблиця для $\underset{\sim}{P}_{SPKПОА}^{p}$

$\underset{\sim}{P}_{32}^{\tau_f p}$	$\mu_{32g}^{p}\ (g=\overline{1,9})$								
	μ_{321}^{p}	μ_{322}^{p}	μ_{323}^{p}	μ_{324}^{p}	μ_{325}^{p}	μ_{326}^{p}	μ_{327}^{p}	μ_{328}^{p}	μ_{329}^{p}
	0	0,2	0,5	0,7	1	0,7	0,5	0,2	0
$\underset{\sim}{P}_{SPKПОА}^{\tau_f p}$	0,03	0,03	0,03	0,038	0,05	0,15	0,15	0,15	0,15

Наступним, відповідно до [20], сформуємо характерні ознаки (ХО):

$$\mathbf{XP_{31}^{1}} = \{\bigcup_{s=1}^{5} XP_{31s}^{1}\} = \{XP_{311}^{1},\ XP_{312}^{1},\ XP_{313}^{1},\ XP_{314}^{1},\ XP_{315}^{1}\} = \{h(\underset{\sim}{T}_{311}^{ep},\ \underset{\sim}{P}_{31}^{\tau_f p}),\ h(\underset{\sim}{T}_{312}^{ep},\ \underset{\sim}{P}_{31}^{\tau_f p}),\ h(\underset{\sim}{T}_{313}^{ep},\ \underset{\sim}{P}_{31}^{\tau_f p}),\ h(\underset{\sim}{T}_{314}^{ep},\ \underset{\sim}{P}_{31}^{\tau_f p}),\ h(\underset{\sim}{T}_{315}^{ep},\ \underset{\sim}{P}_{31}^{\tau_f p})\} = \{0{,}478;\ 1{,}327;\ 3{,}575;\ 7{,}058;\ 8{,}962\};$$

$$\mathbf{XP_{32}^{1}} = \{\bigcup_{s=1}^{3} XP_{32s}^{1}\} = \{XP_{321}^{1},\ XP_{322}^{1},\ XP_{323}^{1}\} = \{h(\underset{\sim}{T}_{321}^{ep},\ \underset{\sim}{P}_{32}^{\tau_f p}),\ h(\underset{\sim}{T}_{322}^{ep},\ \underset{\sim}{P}_{32}^{\tau_f p}),\ h(\underset{\sim}{T}_{323}^{ep},\ \underset{\sim}{P}_{32}^{\tau_f p})\} = \{1{,}228;\ 3{,}518;\ 4{,}878\}.$$

Далі, визначення $IX_{31NUM_{31}}^{1}$ та $IX_{32NUM_{32}}^{1}$ здійснюється за допомогою функції $F^{1}(\mathbf{XP_{31}^{1}})$ і $F^{1}(\mathbf{XP_{32}^{1}})$, яка реалізує пошук мінімального значення із членів підмножини $\mathbf{XP_{31}^{1}}$ та $\mathbf{XP_{32}^{1}}$ відповідно до [20], тобто:

$$IX_{31NUM_{31}}^{1} = \bigwedge_{s=1}^{5} XP_{31s}^{1} = XP_{311}^{1} \wedge XP_{312}^{1} \wedge XP_{313}^{1} \wedge XP_{314}^{1} \wedge XP_{315}^{1} = 0{,}478 \wedge 1{,}327 \wedge 3{,}575 \wedge 7{,}058 \wedge 8{,}962 = XP_{311}^{1} = 0{,}478;$$

$$IX_{32NUM_{32}}^{1} = \bigwedge_{s=1}^{3} XP_{32s}^{1} = XP_{321}^{1} \wedge XP_{322}^{1} \wedge XP_{323}^{1} = 1{,}228 \wedge 3{,}518 \wedge 4{,}878 = XP_{321}^{1} = 1{,}228.$$

Виходячи з обчислень видно, що ідентифікуючим в $\mathbf{T_{31}^{e}}$ буде терм $\underset{\sim}{T}_{311}^{e} = \underset{\sim}{OM}_{31}^{e}$, а відповідне йому перетворене еталонне є $\underset{\sim}{T}_{311}^{ep} = \underset{\sim}{T}_{SPKОП\,1}^{ep} = \underset{\sim}{OM}_{31}^{ep}$ [20].

Фактично, обчислення показують, що $XP_{311}^{1} = 0{,}478$, отже перетворене НЧ $\underset{\sim}{P}_{31}^{\tau_f p} = \underset{\sim}{P}_{SPKОП}^{\tau_f p}$ поточного підсередовища ($\mathbf{P_i^{\tau_f}} = \mathbf{P_3^{\tau_f}} = \mathbf{P_{SP}^{\tau_f}}$) найбільш близько розташоване до перетвореного НЧ $\underset{\sim}{T}_{311}^{ep} = \underset{\sim}{OM}_{31}^{ep}$ еталонного підсередовища ($\mathbf{T_i^{e}} = \mathbf{T_3^{e}} = \mathbf{T_{SP}^{e}}$). А оскільки $\underset{\sim}{P}_{SPKОП}^{\tau_f p}$ та $\underset{\sim}{OM}_{31}^{ep}$ є відображенням $\underset{\sim}{P}_{SPKОП}^{\tau_f p}$ та $\underset{\sim}{OM}_{31}^{e}$, то НЧ $\underset{\sim}{P}_{SPKОП}^{\tau_f p}$ найближче розташоване до НЧ $\underset{\sim}{OM}_{31}^{e}$ еталонного підсередовища ($\mathbf{T_i^{e}} = \mathbf{T_3^{e}} = \mathbf{T_{SP}^{e}}$).

Аналогічно, ідентифікуючим в $\mathbf{T_{32}^{e}}$ є значення $\underset{\sim}{T}_{321}^{e} = \underset{\sim}{M}_{32}^{e}$ та, при цьому, $\underset{\sim}{T}_{321}^{ep} = \underset{\sim}{T}_{SPKПОА\,1}^{ep} = \underset{\sim}{M}_{32}^{ep}$.

Також, враховуючи, що $XP^1_{321} = 1{,}228$, то перетворене НЧ $\underset{\sim}{P}^{\tau_f p}_{32} = \underset{\sim}{P}^{\tau_f p}_{SPКПОА}$ поточного підсередовища ($\mathbf{P}^{\tau_f}_{\mathbf{i}} = \mathbf{P}^{\tau_f}_{\mathbf{3}} = \mathbf{P}^{\tau_f}_{\mathbf{SP}}$) найближче до перетвореного НЧ $\underset{\sim}{T}^{ep}_{321} = \underset{\sim}{M}^{ep}_{32}$ еталонного підсередовища ($\mathbf{T}^{\mathbf{e}}_{\mathbf{i}} = \mathbf{T}^{\mathbf{e}}_{\mathbf{3}} = \mathbf{T}^{\mathbf{e}}_{\mathbf{SP}}$).

І, отже, якщо $\underset{\sim}{P}^{\tau_f p}_{SPКПОА}$ та $\underset{\sim}{M}^{ep}_{32}$ є відображенням $\underset{\sim}{P}^{\tau_f p}_{SPКПОА}$ та $\underset{\sim}{M}^{e}_{32}$, то $\underset{\sim}{P}^{\tau_f p}_{SPКПОА}$ є найближчим до $\underset{\sim}{M}^{e}_{32}$.

Відповідно до [20, 25] наступним за ідентифікуючим для $\mathbf{T}^{\mathbf{e}}_{\mathbf{31}}$ буде слідувати терм з $XP^1_{312} = 1{,}327$, тобто це $\underset{\sim}{T}^{e}_{312}$, який і є допоміжним, а для $\mathbf{T}^{\mathbf{e}}_{\mathbf{32}}$ – буде терм з $XP^1_{322} = 3{,}518$, тобто $\underset{\sim}{T}^{e}_{322}$.

Далі, з урахуванням [20] та допоміжних термів XP^1_{312} і XP^1_{322} розрахуємо нормуючі коефіцієнти:

$$k_{31} = 1/(XP^1_{311} + XP^1_{312}) = 1/(0{,}478 + 1{,}327) = 0{,}554,$$

а також:

$$k_{32} = 1/(XP^1_{321} + XP^1_{322}) = 1/(1{,}228 + 3{,}518) = 0{,}211.$$

На основі [25] обчислимо експертні коефіцієнти параметрів $(P_{31} = P_{SPКОП} = КОП$ та $P_{32} = P_{SPКПОА} = КПОА)$:

$$EC^{min}_{31} = 1 - k_{31} \cdot XP^1_{312},\ EC^{max}_{31} = 1 - k_{31} \cdot XP^1_{311},$$

$$EC^{min}_{31} = 1 - 0{,}554 \cdot 1{,}327 = 0{,}265,$$

$$EC^{max}_{31} = 1 - 0{,}554 \cdot 0{,}478 = 0{,}735 \text{ та}$$

$$EC^{min}_{32} = 1 - k_{32} \cdot XP^1_{322},\ EC^{max}_{32} = 1 - k_{32} \cdot XP^1_{321},$$

$$EC^{min}_{32} = 1 - 0{,}211 \cdot 3{,}518 = 0{,}258,$$

$$EC^{max}_{32} = 1 - 0{,}211 \cdot 1{,}228 = 0{,}741.$$

Зазначимо, що $EC^{max}_{31} = 0{,}735$ та $EC^{max}_{32} = 0{,}741$ будуть відображати рівень упевненості експерта щодо значень сформованих поточних величин $\underset{\sim}{P}^{\tau_f p}_{31}$ і $\underset{\sim}{P}^{\tau_f p}_{32}$ відносно їх еталонних термів, що, відповідно, входять до $\mathbf{T}^{\mathbf{e}}_{\mathbf{31}}$ і $\mathbf{T}^{\mathbf{e}}_{\mathbf{32}}$.

З урахуванням [25] розрахуємо експертний коефіцієнт кібератаки ($\mathbf{CA}^{\tau_f}_{\mathbf{3}} = \mathbf{CA}^{\tau_f}_{\mathbf{SP}} = \mathbf{SP}^{\tau_f}$):

$$EC^{CA}_{3} = (EC^{max}_{31} + EC^{max}_{32})/2 = (0{,}735 + 0{,}741)/2 = 0{,}738.$$

З використанням [21] та отриманих експертних коефіцієнтів параметрів $(EC^{max}_{31},\ EC^{max}_{32})$ і кібератаки (EC^{CA}_{3}) визначимо умовний вираз з підмножини $\mathbf{DR_{3\ 13}}$ (див. приклад в [21]) детекційного підсередовища ($\mathbf{DR_{SP}}$) для виявлення спуфінгу, який буквально можна інтерпретувати, як: «Якщо поточний параметр «Кількість одночасних підключень до сервера» в момент часу τ_f найближчий до значення еталону «Дуже мале» (з експертним коефіцієнтом $0{,}735$) і поточний параметр «Кількість пакетів з однаковою адресою відправника та одержувача» в момент часу τ_f найближчий до значення еталону «Мале» (з експертним коефіцієнтом $0{,}741$), то рівень аномального стану, породженого спуфінгом буде «Низьким» (з експертним коефіцієнтом кібератаки $0{,}738$)», а з урахуванням [21] можна застосувати еквівалентний запис:

$$\begin{gathered} if \\ (E(NUM_{SPКОП},\ 1)\big|_{0{,}735} \wedge E(NUM_{SPКПОА},\ 1)\big|_{0{,}741}) \\ then\ "H"\big|_{0{,}738}. \end{gathered}$$

Як бачимо, для виявлення спуфінгу із підмножини $\mathbf{DR_{3\ 13}}$ був застосований умовний вираз з ідентифікатором (ІД) аномальності «Низький».

На рис. 3 графічно показаний поточний блок (у вигляді заштрихованої прямокутної області, яка утворена за допомогою $\underset{\sim}{P}^{\tau_f}_{31}$ і $\underset{\sim}{P}^{\tau_f}_{32}$) з ІД аномальності «Низький», який інтерпретує аномалію у 2-вимірному параметричному КОП-КПОА-підсередовищі ($\mathbf{P_i} = \mathbf{P_3} = \mathbf{P_{SP}}$), породжену відповідним атакуючим SP-середовищем ($\mathbf{CA}^{\tau_f}$) в момент часу τ_f.

Відповідно до наведеного прикладу видно, що при мінімальному рівні загроз програмна модель СВК ідентифікує аномальний стан, що може бути породжений спуфінгом, як «Низький».

Це відповідає адекватній реакції СВК на мінімальний вплив загроз РІС.

Розглянемо наступний приклад, для якого сформуємо значення величин $\underset{\sim}{P}^{\tau_f}_{SPКОП}$ та $\underset{\sim}{P}^{\tau_f}_{SPКПОА}$ поточного підсередовища ($\mathbf{P}^{\tau_f}_{\mathbf{i}} = \mathbf{P}^{\tau_f}_{\mathbf{3}}$) атакуючого середовища ($\mathbf{CA}^{\tau_f}$), що несе незначну (дещо вищого мінімального рівня) загрозу ФС:

$\underset{\sim}{P}^{\tau_f}_{SPKO\Pi} = \{0/0,2;\ 0,4/0,2;\ 1/0,42;\ 0,2/0,75;\ 0/0,75\}$;

$\underset{\sim}{P}^{\tau_f}_{SPK\Pi OA} = \{0/0,05;\ 0,5/0,05;\ 1/0,3;\ 0,7/0,5;\ 0/0,5\}$.

Далі, відповідно до номіналізованих НЧ еталонного підсередовища ($\mathbf{T_i^e} = \mathbf{T_3^e} = \mathbf{T_{SP}^e}$), здійснимо формування номіналізованого НЧ поточного підсередовища ($\mathbf{P_i^{\tau_f}} = \mathbf{P_3^{\tau_f}}$) з урахуванням [19], тобто

$$\underset{\sim}{P}^{\tau_f p}_{31} = \{\bigcup_{g=1}^{13} \mu^p_{31g} / x^p_{31g}\} = \{\mu^p_{311} / x^p_{311},\ \mu^p_{312} / x^p_{312},$$
$$\mu^p_{313} / x^p_{313},\ \mu^p_{314} / x^p_{314},\ \mu^p_{315} / x^p_{315},$$
$$\mu^p_{316} / x^p_{316},\ \mu^p_{317} / x^p_{317},\ \mu^p_{318} / x^p_{318},\ \mu^p_{319} / x^p_{319},$$
$$\mu^p_{31(10)} / x^p_{31(10)},$$
$$\mu^p_{31(11)} / x^p_{31(11)},\ \mu^p_{31(12)} / x^p_{31(12)},\ \mu^p_{31(13)} / x^p_{31(13)}\},$$

де:

- $\mu^p_{311} = \mu^p_{31(13)} = AL_{311} = 0$,
- $\mu^p_{312} = \mu^p_{31(12)} = AL_{312} = 0,2$,
- $\mu^p_{313} = \mu^p_{31(11)} = AL_{313} = 0,3$,
- $\mu^p_{314} = \mu^p_{31(10)} = AL_{314} = 0,4$,

  $\mu^p_{315} = \mu^p_{319} = AL_{315} = 0,6$,
- $\mu^p_{316} = \mu^p_{318} = AL_{316} = 0,7$,
- $\mu^p_{317} = \mu^p_{317} = AL_{317} = 1$,
- $\mu^p_{311} = \mu_{311} = 0$,
- $x^p_{311} = x_{311} = 0,2$.

$$\underset{\sim}{P}^{\tau_f p}_{32} = \{\bigcup_{g=1}^{9} \mu^p_{32g} / x^p_{32g}\} =$$
$$\{\mu^p_{321} / x^p_{321},\ \mu^p_{322} / x^p_{322},\ \mu^p_{323} / x^p_{323},\ \mu^p_{324} / x^p_{324},$$
$$\mu^p_{325} / x^p_{325},\ \mu^p_{326} / x^p_{326},\ \mu^p_{327} / x^p_{327},\ \mu^p_{328} / x^p_{328},$$
$$\mu^p_{329} / x^p_{329}\},$$

де:

- $\mu^p_{321} = \mu^p_{329} = AL_{321} = 0$,
- $\mu^p_{322} = \mu^p_{328} = AL_{322} = 0,2$,
- $\mu^p_{323} = \mu^p_{327} = AL_{323} = 0,5$,
- $\mu^p_{324} = \mu^p_{326} = AL_{324} = 0,7$,
- $\mu^p_{325} = \mu^p_{325} = AL_{325} = 1$,
- $\mu^p_{321} = \mu_{321} = 0$,
- $x^p_{321} = x_{321} = 0,05$.

Далі, формування номіналізованого НЧ $\underset{\sim}{P}^{\tau_f p}_{ij} = \underset{\sim}{P}^{\tau_f p}_{31}$ поточного підсередовища ($\mathbf{P_i^{\tau_f}} = \mathbf{P_3^{\tau_f}}$) здійснюється відповідно до [19] за допомогою α--рівневих інтервалів $\mathbf{AL^{Ip}_{31}}$ при $\rho = 5$ і

$$\mu_{31max} = \bigvee_{q=1}^{\rho} \mu_{31q} = \mu_{311} \vee \mu_{312} \vee \mu_{313} \vee \mu_{314} \vee \mu_{315} =$$
$$0 \vee 0,4 \vee 1 \vee 0,2 \vee 0 = \mu_{313} = 1$$

та якщо:

- $r_1 = 1,\ c = \overline{1,k_1},\ k_1 = 3$ і

  $(\mu_{311} < AL^{Ip}_{311c} \le \mu_{312}) \wedge (x_{312} \le x_{31max})$

  $((0 < AL^{Ip}_{311c} \le 0,4) \wedge (0,2 \le 0,42))$, то

$$\mathbf{AL^{Ip}_{311}} = \{\bigcup_{c=1}^{k_1} AL^{Ip}_{311c}\} = \{AL^{Ip}_{3111},\ AL^{Ip}_{3112},\ AL^{Ip}_{3113}\} = \{0,2;\ 0,3;\ 0,4\};$$

- $r_2 = 2,\ c = \overline{1,k_2},\ k_2 = 3$,

  $(\mu_{312} < AL^{Ip}_{312c} \le \mu_{313}) \wedge (x_{313} \le x_{31max})$

  $((0,4 < AL^{Ip}_{312c} \le 1) \wedge ,(0,42 \le 0,42))$, то

$$\mathbf{AL^{Ip}_{312}} = \{\bigcup_{c=1}^{k_2} AL^{Ip}_{312c}\} = \{AL^{Ip}_{3121},\ AL^{Ip}_{3122},\ AL^{Ip}_{3123}\} = \{0,6;\ 0,7;\ 1\};$$

- $r_3 = 3,\ c = \overline{1,k_3},\ k_3 = 5$,

  $(\mu_{313} > AL^{Ip}_{313c} \ge \mu_{314}) \wedge (x_{314} \ge x_{31max})$

  $((1 > AL^{Ip}_{313c} \ge 0,2) \wedge (0,75 \ge 0,42))$, то

$$\mathbf{AL^{Ip}_{313}} = \{\bigcup_{c=1}^{k_3} AL^{Ip}_{313c}\} = \{AL^{Ip}_{3131},\ AL^{Ip}_{3132},\ AL^{Ip}_{3133},\ AL^{Ip}_{3134},\ AL^{Ip}_{3135}\} = \{0,7;\ 0,6;\ 0,4;\ 0,3;\ 0,2\};$$

- $r_4 = 4,\ c = \overline{1,k_4},\ k_4 = 1$,

  $(\mu_{314} > AL^{Ip}_{314c} \ge \mu_{315}) \wedge (x_{315} \ge x_{31max})$

  $((0,2 > AL^{Ip}_{314c} \ge 1) \wedge (0,75 \ge 0,42))$, то

$$\mathbf{AL^{Ip}_{314}} = \{\bigcup_{c=1}^{k_4} AL^{Ip}_{314c}\} = \{AL^{Ip}_{3141}\} = \{0\}.$$

З урахуванням обчислених значень, отримаємо наступний вигляд:

$$\mathbf{AL^{Ip}_{31}} = \{\bigcup_{b=1}^{\rho-1}\{\bigcup_{c=1}^{k_b} AL^{Ip}_{31bc}\}\} =$$
$$\{\{AL^{Ip}_{3111},\ AL^{Ip}_{3112},\ AL^{Ip}_{3113}\},\ \{AL^{Ip}_{3121},\ AL^{Ip}_{3122},\ AL^{Ip}_{3123}\},$$
$$\{AL^{Ip}_{3131},\ AL^{Ip}_{3132},\ AL^{Ip}_{3133},\ AL^{Ip}_{3134},\ AL^{Ip}_{3135}\},$$
$$\{AL^{Ip}_{3141}\}\} =$$
$$\{\{0,2;\ 0,3;\ 0,4\},\ \{0,6;\ 0,7;\ 1\},$$
$$\{0,7;\ 0,6;\ 0,4;\ 0,3;\ 0,2\},\ \{0\}\}.$$

За аналогією з прикладом для $\underset{\sim}{P}^{\tau_f p}_{31}$, формування номіналізованого НЧ $\underset{\sim}{P}^{\tau_f p}_{ij} = \underset{\sim}{P}^{\tau_f p}_{32}$ поточного підсередовища ($\mathbf{P}_i^{\tau_f} = \mathbf{P}_3^{\tau_f}$) реалізується на основі [19] за допомогою α-рівневих інтервалів $\mathbf{AL}_{32}^{\mathbf{lp}}$, тобто $\mathbf{AL}_{32}^{\mathbf{lp}} = \{\bigcup_{b=1}^{\rho-1}\{\bigcup_{c=1}^{k_b} AL_{32bc}^{lp}\}\} = \{\{AL_{3211}^{lp}, AL_{3212}^{lp}\}, \{AL_{3221}^{lp}, AL_{3222}^{lp}\}, \{AL_{3231}^{lp}\}, \{AL_{3241}^{lp}, AL_{3242}^{lp}, AL_{3243}^{lp}, AL_{3244}^{lp}\}\} = \{\{0,2;\ 0,5\}, \{0,7;\ 1\}, \{0,7\}, \{0,5; 0,2; 1\}\}$.

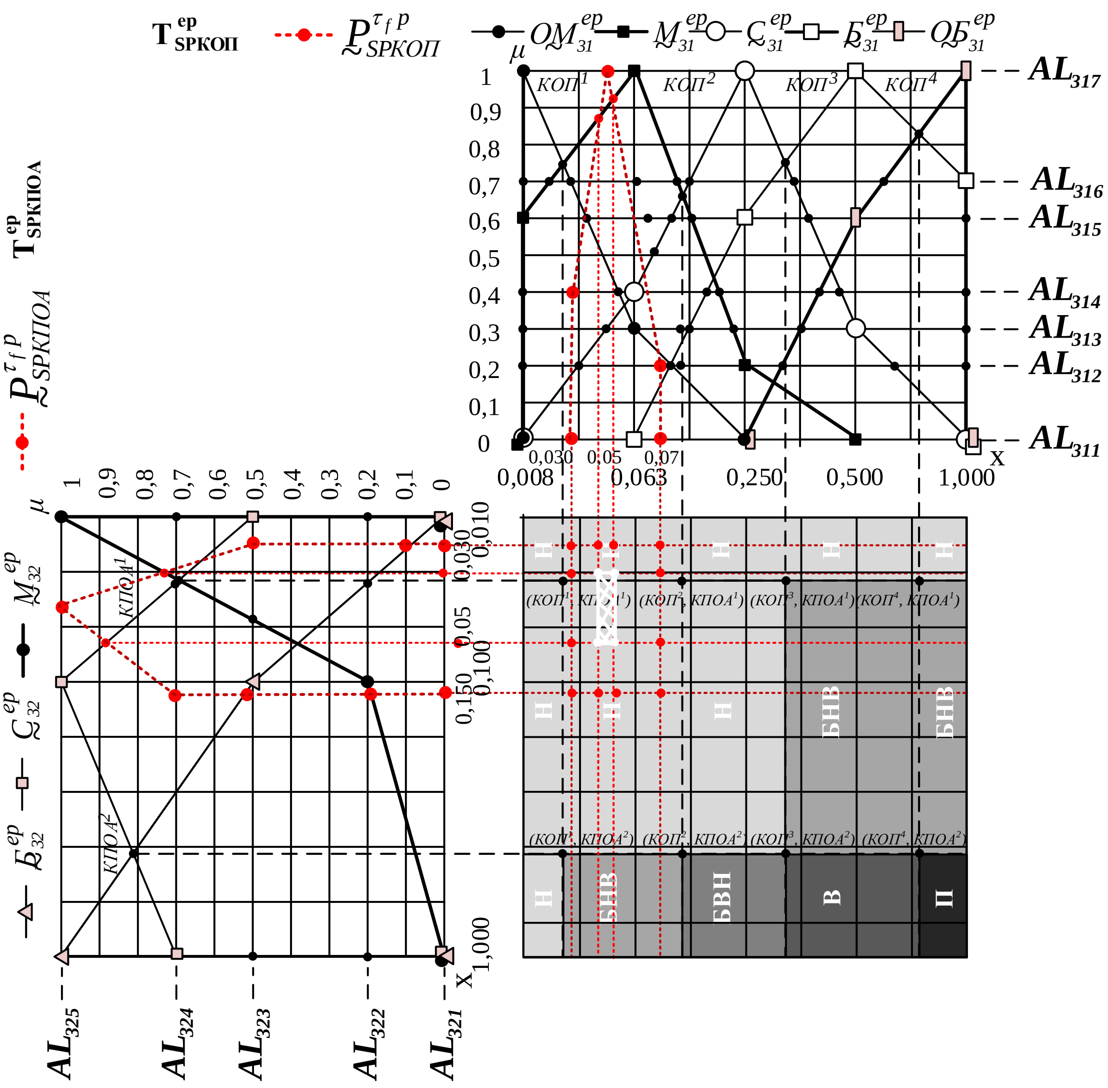

Рис. 3. Графічна інтерпретація поточного блоку відносно фазифікованих значень $\underset{\sim}{P}_{31}^{\tau_f}$ і $\underset{\sim}{P}_{32}^{\tau_f}$ з ІД «Низький», який інтерпретує аномалію у КОП-КПОА-підсередовищі, породжену SP-середовищем

Обчислення значень x_{31g}^{p} для перетворених НЧ $\underset{\sim}{P}_{31}^{\tau_f p} = \underset{\sim}{P}_{SPКОП}^{\tau_f p}$ поточного підсередовища ($\mathbf{P}_i^{\tau_f} = \mathbf{P}_3^{\tau_f}$) здійснюється аналогічно до кроку 4 [19] при $z = 13$, $g = \overline{2,13}$ на основі компонентів μ_{ijg} / x_{ijg} (див. приклад етапу 3 в [19]), тобто

$\mu_{311} = 0$, $\mu_{312} = 0,4$, $x_{311} = 0,2$ та $x_{312} = 0,2$.

Далі, з урахуванням цього:

- якщо $\mu_{312}^{p} = AL_{312}^{lp} = 0,2$, то

$x_{312}^{p} = 0,2 + ((0,2 - 0) \cdot (0,2 - 0,2)) / (0,4 - 0) = 0,2$;

- якщо $\mu_{313}^{p} = AL_{313}^{lp} = 0,3$, то

$x_{313}^{p} = 0,2 + ((0,3 - 0) \cdot (0,2 - 0,2)) / (0,4 - 0) = 0,2$;

- якщо $\mu_{314}^{p} = AL_{314}^{lp} = 0,4$, то

$x_{314}^{p} = 0,2 + ((0,4 - 0) \cdot (0,2 - 0,2)) / (0,4 - 0) = 0,2$.

Наступним, при $\mu_{312} = 0,4$, $\mu_{313} = 1$, $x_{312} = 0,2$ та $x_{313} = 0,42$:

- якщо $\mu_{315}^{p} = AL_{315}^{lp} = 0,6$, то

$x_{315}^{p} = 0,2 + ((0,6 - 0,4) \cdot (0,42 - 0,2)) / (1 - 0,4) = 0,27$;

- якщо $\mu^p_{316} = AL^{Ip}_{316} = 0{,}7$, то

$x^p_{316} = 0{,}2 + ((0{,}7 - 0{,}4)\cdot(0{,}42 - 0{,}2))/(1 - 0{,}4) = 0{,}31$;

- якщо $\mu^p_{317} = AL^{Ip}_{317} = 1$, то

$x^p_{317} = 0{,}2 + ((1 - 0{,}4)\cdot(0{,}42 - 0{,}2))/(1 - 0{,}4) = 0{,}42$.

Далі, при $\mu_{313} = 1$, $\mu_{314} = 0{,}2$, $x_{313} = 0{,}42$ та $x_{314} = 0{,}75$:

- якщо $\mu^p_{318} = AL^{Ip}_{318} = 0{,}7$, то

$x^p_{318} = 0{,}2 + ((0{,}7 - 1)\cdot(0{,}75 - 0{,}42))/(0{,}2 - 1) = 0{,}324$;

- якщо $\mu^p_{319} = AL^{Ip}_{319} = 0{,}6$, то

$x^p_{319} = 0{,}2 + ((0{,}6 - 1)\cdot(0{,}75 - 0{,}42))/(0{,}2 - 1) = 0{,}365$;

- якщо $\mu^p_{31(10)} = AL^{Ip}_{31(10)} = 0{,}4$ то

$x^p_{31(10)} = 0{,}2 + ((0{,}4 - 1)\cdot(0{,}75 - 0{,}42))/(0{,}2 - 1) = 0{,}448$;

- якщо $\mu^p_{31(11)} = AL^{Ip}_{31(11)} = 0{,}3$, то

$x^p_{31(11)} = 0{,}2 + ((0{,}3 - 1)\cdot(0{,}75 - 0{,}42))/(0{,}2 - 1) = 0{,}489$;

- якщо $\mu^p_{31(12)} = AL^{Ip}_{31(12)} = 0{,}2$, то

$x^p_{31(12)} = 0{,}2 + ((0{,}2 - 1)\cdot(0{,}75 - 0{,}42))/(0{,}2 - 1) = 0{,}53$.

Наступним, при $\mu_{314} = 0{,}2$, $\mu_{315} = 0$, $x_{314} = 0{,}75$ та $x_{315} = 0{,}75$ для $\mu^{ep}_{31(13)} = AL^{Ip}_{31(13)} = 0$ визначимо

$$x^{ep}_{31(13)} = 0{,}75 + ((0 - 0{,}2)\cdot(0{,}75 - 0{,}75))/(0 - 0{,}2) = 0{,}75,$$

а $\mu^p_{311} = \mu_{311} = 0$, $x^p_{311} = x_{311} = 0{,}2$.

Таким чином, номіналізоване НЧ поточного підсередовища ($\mathbf{P}^{\tau_f}_{\mathbf{i}} = \mathbf{P}^{\tau_f}_{\mathbf{3}}$) відповідно до [19] приймає вигляд:

$$\underset{\sim}{P}^{\tau_f p}_{31} = \underset{\sim}{P}^{\tau_f p}_{SPKOП} = \{0/0{,}2;\ 0{,}2/0{,}2;\ 0{,}3/0{,}2;\ 0{,}4/0{,}2;\ 0{,}6/0{,}27;\ 0{,}7/0{,}31;\ 1/0{,}42;\ 0{,}7/0{,}324;\ 0{,}6/0{,}365;\ 0{,}4/0{,}448;\ 0{,}3/0{,}489;\ 0{,}2/0{,}53;\ 0/0{,}75\}.$$

Таблиця 3

Узагальнювальна таблиця для $\underset{\sim}{P}^{p}_{SPKOП}$

$\underset{\sim}{P}^{\tau_f p}_{31}$	μ^p_{31g} $(g = \overline{1,13})$												
	μ^p_{311}	μ^p_{312}	μ^p_{313}	μ^p_{314}	μ^p_{315}	μ^p_{316}	μ^p_{317}	μ^p_{318}	μ^p_{319}	$\mu^p_{31(10)}$	$\mu^p_{31(11)}$	$\mu^p_{31(12)}$	$\mu^p_{31(13)}$
	0	0,2	0,3	0,4	0,6	0,7	1	0,7	0,6	0,4	0,3	0,2	0
$\underset{\sim}{P}^{\tau_f p}_{SPKOП}$	0,2	0,2	0,2	0,2	0,27	0,31	0,42	0,324	0,365	0,448	0,489	0,53	0,75

Таблиця 4

Узагальнювальна таблиця для $\underset{\sim}{P}^{p}_{SPKПОА}$

$\underset{\sim}{P}^{\tau_f p}_{32}$	μ^p_{32g} $(g = \overline{1,9})$								
	μ^p_{321}	μ^p_{322}	μ^p_{323}	μ^p_{324}	μ^p_{325}	μ^p_{326}	μ^p_{327}	μ^p_{328}	μ^p_{329}
	0	0,2	0,5	0,7	1	0,7	0,5	0,2	0
$\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$	0,05	0,05	0,05	0,15	0,3	0,5	0,5	0,5	0,5

Обчислення значень x^p_{36g} для перетворених НЧ $\underset{\sim}{P}^{\tau_f p}_{32} = \underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ поточного підсередовищам ($\mathbf{P}^{\tau_f}_{\mathbf{i}} = \mathbf{P}^{\tau_f}_{\mathbf{3}} = \mathbf{P}^{\tau_f}_{\mathbf{SP}}$) здійснюється аналогічно, з урахуванням [19], при $z = 9$ за допомогою компонентів μ_{ijg} / x_{ijg} (див. приклад етапу 3 в [19]), тобто при $\mu_{321} = 0$, $\mu_{322} = 0{,}5$, $x_{321} = 0{,}05$ та $x_{322} = 0{,}05$.

Далі, з урахуванням цих значень:

- якщо $\mu^p_{322} = AL^{Ip}_{322} = 0{,}2$, то $x^p_{322} = 0{,}05$;
- якщо $\mu^p_{323} = AL^{Ip}_{323} = 0{,}5$, то $x^p_{323} = 0{,}05$.

При $\mu_{322} = 0{,}5$, $\mu_{323} = 1$, $x_{322} = 0{,}05$ та $x_{323} = 0{,}3$:

- якщо $\mu^p_{324} = AL^{Ip}_{324} = 0{,}7$, то $x^p_{324} = 0{,}15$;
- якщо $\mu^p_{325} = AL^{Ip}_{325} = 1$, то $x^p_{325} = 0{,}3$.

Наступним, при $\mu_{323} = 1$, $\mu_{324} = 0{,}7$, $x_{323} = 0{,}3$ та $x_{324} = 0{,}5$ для $\mu^p_{326} = AL^{Ip}_{326} = 0{,}7$ обчислимо $x^p_{326} = 0{,}5$

І, нарешті, при $\mu_{324} = 0{,}7$, $\mu_{325} = 0$, $x_{324} = 0{,}5$ та $x_{325} = 0{,}5$ для $\mu^p_{327} = AL^{Ip}_{327} = 0{,}5$, $\mu^p_{328} = AL^{Ip}_{328} = 0{,}2$, $\mu^p_{329} = AL^{Ip}_{329} = 0$, відповідно обчислимо

$$x^p_{327} = x^p_{328} = x^p_{329} = 0{,}5, \text{ а } \mu^p_{321} = \mu_{321} = 0,$$
$$x^p_{321} = x_{321} = 0{,}05.$$

Таким чином, номіналізоване НЧ поточного підсередовища ($\mathbf{P}^{\tau_f}_{\mathbf{i}} = \mathbf{P}^{\tau_f}_{\mathbf{3}} = \mathbf{P}^{\tau_f}_{\mathbf{SP}}$) відповідно до [19] має вигляд : $\underset{\sim}{P}^{\tau_f p}_{32} = \underset{\sim}{P}^{\tau_f p}_{SPKПОА} = \{0/0{,}05;\ 0{,}2/0{,}05;\ 0{,}5/0{,}05;\ 0{,}7/0{,}15;\ 1/0{,}3;\ 0{,}7/0{,}5;\ 0{,}5/0{,}5;\ 0{,}2/0{,}5;\ 0/0{,}5\}$.

Зведемо отримані дані до узагальнювальних табл. 3-4.

Далі, відповідно до [20], сформуємо ХО:

$\mathbf{XP^1_{31}} = \{\bigcup_{s=1}^{5} XP^1_{31s}\} = \{XP^1_{311},\ XP^1_{312},\ XP^1_{313},\ XP^1_{314},\ XP^1_{315}\} = \{h(\underset{\sim}{T}^{ep}_{311},\ \underset{\sim}{P}^{\tau_f p}_{31}),\ h(\underset{\sim}{T}^{ep}_{312},\ \underset{\sim}{P}^{\tau_f p}_{31}),\ h(\underset{\sim}{T}^{ep}_{313},\ \underset{\sim}{P}^{\tau_f p}_{31}),\ h(\underset{\sim}{T}^{ep}_{314},\ \underset{\sim}{P}^{\tau_f p}_{31}),\ h(\underset{\sim}{T}^{ep}_{315},\ \underset{\sim}{P}^{\tau_f p}_{31})\} = \{4{,}086;\ 3{,}111;\ 1{,}587;\ 3{,}464;\ 4{,}794\}$;

$\mathbf{XP^1_{32}} = \{\bigcup_{s=1}^{3} XP^1_{32s}\} = \{XP^1_{321},\ XP^1_{322},\ XP^1_{323}\} = \{h(\underset{\sim}{T}^{ep}_{321},\ \underset{\sim}{P}^{\tau_f p}_{32}),\ h(\underset{\sim}{T}^{ep}_{322},\ \underset{\sim}{P}^{\tau_f p}_{32}),\ h(\underset{\sim}{T}^{ep}_{323},\ \underset{\sim}{P}^{\tau_f p}_{32})\} = \{2{,}25;\ 2{,}424;\ 3{,}104\}$.

Далі, визначення $IX^1_{31NUM_{31}}$ та $IX^1_{32NUM_{32}}$ здійснюється за допомогою функції $F^1(\mathbf{XP^1_{31}})$ і $F^1(\mathbf{XP^1_{32}})$, яка реалізує пошук мінімального значення із членів підмножини $\mathbf{XP^1_{31}}$ та $\mathbf{XP^1_{32}}$ відповідно до [20], тобто:

$$IX^{1}_{31\,NUM_{31}} = \bigwedge_{s=1}^{5} XP^{1}_{31s} =$$

$XP^{1}_{311} \wedge XP^{1}_{312} \wedge XP^{1}_{313} \wedge XP^{1}_{314} \wedge XP^{1}_{315} = 4{,}086 \wedge 3{,}111 \wedge 1{,}587 \wedge 3{,}464 \wedge 4{,}794 = XP^{1}_{313} = 1{,}587;$

$IX^{1}_{32\,NUM_{32}} = \bigwedge_{s=1}^{3} XP^{1}_{32s} = XP^{1}_{321} \wedge XP^{1}_{322} \wedge XP^{1}_{323} = 2{,}25 \wedge 2{,}424 \wedge 3{,}104 = XP^{1}_{321} = 2{,}25.$

Виходячи з обчислень видно, що ідентифікуючим в $\mathbf{T^{e}_{31}}$ буде терм $\underset{\sim}{T}^{e}_{313} = \underset{\sim}{C}^{e}_{31}$ (див. приклад в [20]), а відповідне йому перетворене еталонне є $\underset{\sim}{T}^{ep}_{313} = \underset{\sim}{T}^{ep}_{SPKOП3} = \underset{\sim}{C}^{ep}_{31}$ (див. приклад етапу 2 в [20]). Фактично, обчислення показують, що $XP^{1}_{313} = 1{,}587$, отже перетворене НЧ $\underset{\sim}{P}^{\tau_f p}_{31} = \underset{\sim}{P}^{\tau_f p}_{SPKOП}$ поточного підсередовища ($\mathbf{P^{\tau_f}_{i} = P^{\tau_f}_{3} = P^{\tau_f}_{SP}}$) найближче розташоване до перетвореного НЧ $\underset{\sim}{T}^{ep}_{313} = \underset{\sim}{C}^{ep}_{31}$ еталонного підсередовища ($\mathbf{T^{e}_{i} = T^{e}_{3} = T^{e}_{SP}}$). А, оскільки, $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$ та $\underset{\sim}{C}^{ep}_{31}$ є відображенням $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$ та $\underset{\sim}{C}^{e}_{31}$, то $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$ найближче розташоване до НЧ $\underset{\sim}{C}^{e}_{31}$ еталонного підсередовища ($\mathbf{T^{e}_{i} = T^{e}_{3} = T^{e}_{SP}}$).

Аналогічно, ідентифікуючим в $\mathbf{T^{e}_{32}}$ є значення $\underset{\sim}{T}^{e}_{321} = \underset{\sim}{M}^{e}_{32}$ (див. приклад в [20]) та, при цьому, $\underset{\sim}{T}^{ep}_{321} = \underset{\sim}{T}^{ep}_{SPKПОА\,1} = \underset{\sim}{M}^{ep}_{32}$ (див. приклад етапу 2 в [20]).

Також, враховуючи, що $XP^{1}_{321} = 2{,}25$, то перетворене НЧ $\underset{\sim}{P}^{\tau_f p}_{32} = \underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ поточного підсередовища ($\mathbf{P^{\tau_f}_{i} = P^{\tau_f}_{3} = P^{\tau_f}_{SP}}$) найближче до перетвореного НЧ $\underset{\sim}{T}^{ep}_{321} = \underset{\sim}{M}^{ep}_{32}$ еталонного підсередовища ($\mathbf{T^{e}_{i} = T^{e}_{3} = T^{e}_{SP}}$). І, отже, якщо $\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ та $\underset{\sim}{M}^{ep}_{32}$ є відображенням $\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ та $\underset{\sim}{M}^{e}_{32}$, то $\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ є найближчим до $\underset{\sim}{M}^{e}_{32}$.

Відповідно до [20] наступним за ідентифікуючим для $\mathbf{T^{e}_{31}}$ буде слідувати терм з $XP^{1}_{312} = 3{,}111$, тобто це $\underset{\sim}{T}^{e}_{312}$, який і є допоміжним, а для $\mathbf{T^{e}_{32}}$ – терм з $XP^{1}_{322} = 2{,}424$, тобто $\underset{\sim}{T}^{e}_{322}$.

Далі, з урахуванням [25] та допоміжних термів XP^{1}_{312} і XP^{1}_{322} розрахуємо нормуючі коефіцієнти:

$$k_{31} = 1/(XP^{1}_{313} + XP^{1}_{312}) = 1/(1{,}587 + 3{,}111) = 0{,}213;$$

$$k_{32} = 1/(XP^{1}_{321} + XP^{1}_{322}) = 1/(2{,}25 + 2{,}424) = 0{,}214.$$

На основі [25] обчислимо експертні коефіцієнти параметрів ($P_{31} = P_{SPKOП} = KOП$ та $P_{32} = P_{SPKПОА} = KПОА$)

$$EC^{min}_{31} = 1 - k_{31} \cdot XP^{1}_{312},$$

$$EC^{max}_{31} = 1 - k_{31} \cdot XP^{1}_{313}, \text{ тобто}$$

$$EC^{min}_{31} = 1 - 0{,}213 \cdot 3{,}111 = 0{,}338,$$

$$EC^{max}_{31} = 1 - 0{,}213 \cdot 1{,}587 = 0{,}662 \text{ та}$$

$$EC^{min}_{32} = 1 - k_{32} \cdot XP^{1}_{322},$$

$$EC^{max}_{32} = 1 - k_{32} \cdot XP^{1}_{321}, \text{ тобто}$$

$$EC^{min}_{32} = 1 - 0{,}214 \cdot 2{,}424 = 0{,}482,$$

$$EC^{max}_{32} = 1 - 0{,}214 \cdot 2{,}25 = 0{,}518.$$

Зазначимо, що $EC^{max}_{31} = 0{,}662$ та $EC^{max}_{32} = 0{,}518$ будуть відображати рівень упевненості експерта щодо значень сформованих поточних величин $\underset{\sim}{P}^{\tau_f p}_{31}$ і $\underset{\sim}{P}^{\tau_f p}_{32}$ відносно їх еталонних термів, що, відповідно, входять до $\mathbf{T^{e}_{31}}$ і $\mathbf{T^{e}_{32}}$.

З урахуванням [25] розрахуємо експертний коефіцієнт кібератаки ($\mathbf{CA^{\tau_f}_{3} = CA^{\tau_f}_{SP} = SP^{\tau_f}}$):

$$EC^{CA}_{3} = (EC^{max}_{31} + EC^{max}_{32})/2 = (0{,}662 + 0{,}518)/2 = 0{,}59.$$

З використанням [21] та отриманих експертних коефіцієнтів параметрів (EC^{max}_{31}, EC^{max}_{32}) і кібератаки (EC^{CA}_{3}) визначимо умовний вираз з підмножини $\mathbf{DR_{3\,13}}$ детекційного підсередовища ($\mathbf{DR_{SP}}$) для виявлення спуфінгу, що інтерпретується, як: «Якщо поточний параметр «Кількість одночасних підключень до сервера» в момент часу τ_f найближчий до значення еталону «Середнє» (з експертним коефіцієнтом $0{,}662$) і поточний параметр «Кількість пакетів з однаковою адресою відправника та одержувача» в момент часу τ_f найближчий до значення еталону «Мале» (з експертним коефіцієнтом $0{,}518$), то рівень аномального стану, породженого спуфінгом буде «Більш низький ніж високий» (з експертним коефіцієнтом кібератаки $0{,}59$)», що з урахуванням [21] можна записати, як:

$$\text{if}$$

$$(E\,(NUM_{SPKOП},\ 3)\big|_{0{,}662} \wedge E\,(NUM_{SPKПОА},\ 1)\big|_{0{,}518})$$

$$\text{then "БНВ"}\big|_{0{,}59}.$$

Із застосованого еквівалентного представлення видно, що для виявлення кібератаки із підмножини $\mathbf{DR_{3\,13}}$ був застосований умовний вираз з ІД аномальності «Більш низький ніж високий».

На рис. 4 графічно показаний поточний блок (у вигляді заштрихованої прямокутної області, яка утворена за допомогою $\underset{\sim}{P}^{\tau_f}_{31}$, $\underset{\sim}{P}^{\tau_f}_{32}$) з ІД аномальності «Більш низький ніж високий», який інтерпретує аномалію у *2*-вимірному параметричному КОП-КПОА-підсередовищі ($\mathbf{P_i{=}P_3{=}P_{SP}}$), породжену відповідним атакуючим SP-середовищем ($\mathbf{CA}^{\tau_f}$) в момент часу τ_f.

Відповідно до наведеного прикладу видно, що при незначному (дещо вищого мінімального) рівні загроз програмна модель СВК ідентифікує аномальний стан, що може бути породжений кібератакою, як «Більш низький ніж високий».

Це відповідає (з урахуванням експертних коефіцієнтів та коефіцієнта кібератаки) адекватній реакції СВК на незначний вплив загроз на РІС.

У наступному прикладі скористаємось сформованими значеннями величин $\underset{\sim}{P}^{\tau_f}_{SPKOП}$ та $\underset{\sim}{P}^{\tau_f}_{SPKПOA}$ поточного підсередовища ($\mathbf{P_i}^{\tau_f} = \mathbf{P_3}^{\tau_f}$) [19, 25], що несе високий рівень загроз ФС:

$$\underset{\sim}{P}^{\tau_f}_{SPKOП} = \{0/0{,}095;\ 0{,}4/0{,}095;\ 1/0{,}28;\ 0{,}2/0{,}58; 0/0{,}58\};$$

$$\underset{\sim}{P}^{\tau_f}_{SPKПOA} = \{0/0{,}082;\ 0{,}5/0{,}082;\ 1/0{,}82;\ 0{,}7/1;\ 0/1\}.$$

З урахуванням [21] та отриманих експертних коефіцієнтів параметрів $(EC^{max}_{31},\ EC^{max}_{32})$ і кібератаки (EC^{CA}_{3}) зазначимо умовний вираз з підмножини $\mathbf{DR}_{3\ 13}$ (див. приклад в [21]) детекційного підсередовища ($\mathbf{DR_{SP}}$) для виявлення спуфінгу: «Якщо поточний параметр «Кількість одночасних підключень до сервера» в момент часу τ_f найближчий до значення еталону «Середнє» (з експертним коефіцієнтом $0{,}713$) і поточний параметр «Кількість пакетів з однаковою адресою відправника та одержувача» в момент часу τ_f найближчий до значення еталону «Велике» (з експертним коефіцієнтом $0{,}741$), то рівень аномального стану, породженого спуфінгом буде «Більш високим ніж низьким» (з експертним коефіцієнтом кібератаки $0{,}727$)». З урахуванням [21] можна застосувати еквівалентний запис:

$$\begin{gathered} \textit{if} \\ (E\,(NUM_{SPKOП},\ 3)\big|_{0{,}713} \wedge E\,(NUM_{SPKПOA},\ 3)\big|_{0{,}741}) \\ \textit{then}\ \text{"БВН"}\big|_{0{,}727}. \end{gathered}$$

Як бачимо, для виявлення кібератаки із підмножини $\mathbf{DR}_{3\ 13}$ був застосований умовний вираз з ІД аномальності «БВН».

На рис. 5 графічно показаний поточний блок (у вигляді заштрихованої прямокутної області, яка утворена за допомогою $\underset{\sim}{P}^{\tau_f}_{31}$, $\underset{\sim}{P}^{\tau_f}_{32}$) з ІД аномальності «Більш високим ніж низьким», який інтерпретує аномалію у КОП-КПОА-підсередовищі ($\mathbf{P_i{=}P_3{=}P_{SP}}$), породжену відповідним атакуючим SP-середовищем ($\mathbf{CA}^{\tau_f}$) в момент часу τ_f. Відповідно до представленого прикладу видно, що при високому рівні загроз СВК ідентифікує аномальний стан, який може бути породжений кібератакою, як «Більш високим ніж низьким».

Це відповідає адекватній реакції програмної моделі СВК високому рівню впливу кібератак на РІС. За результатами експерименту можна зробити висновок, що у всіх випадках модель СВК адекватно реагує на впливи атакуючого середовища.

На основі такого типу програмних розробок можна удосконалювати сучасні СВВ за рахунок додаткової можливості динамічного (у режимі реального часу) контролю стану безпеки ІС відносно реалізованих кібератак та рівнів впливу різних типів загроз на РІС.

Це, також, підтверджується наступними експериментальними даними, що адекватно відображають впливи атакуючого середовища.

За результатами застосування розробленого емулятора та проведеного експериментального дослідження що здійснювалось за допомогою розробленої віртуальної мережі (див. рис. 1), було проведене моделювання 2000 атак (з достатньо високим рівнем впливу на ФС), кожна з яких виявлена за допомогою певного умовного виразу сформованого детекційного середовища, яке у розглянутому випадку складається з одного підсередовища ($\mathbf{DR_3{=}DR_{SP}}$). Результати проведеного експерименту інтегровано в табл. 5.

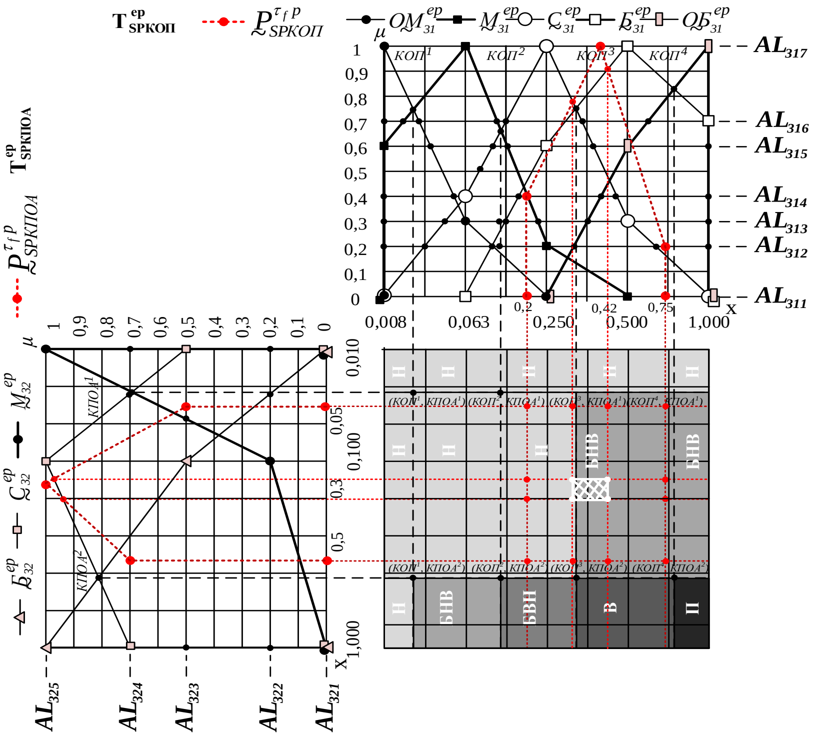

Рис. 4. Графічна інтерпретація поточного блоку відносно фазифікованих значень $\underset{\sim}{P}_{31}^{\tau_f}$ і $\underset{\sim}{P}_{32}^{\tau_f}$ з ІД «Більш низький ніж високий», який інтерпретує аномалію у КОП-КПОА-підсередовищі, породжену SP-середовищем

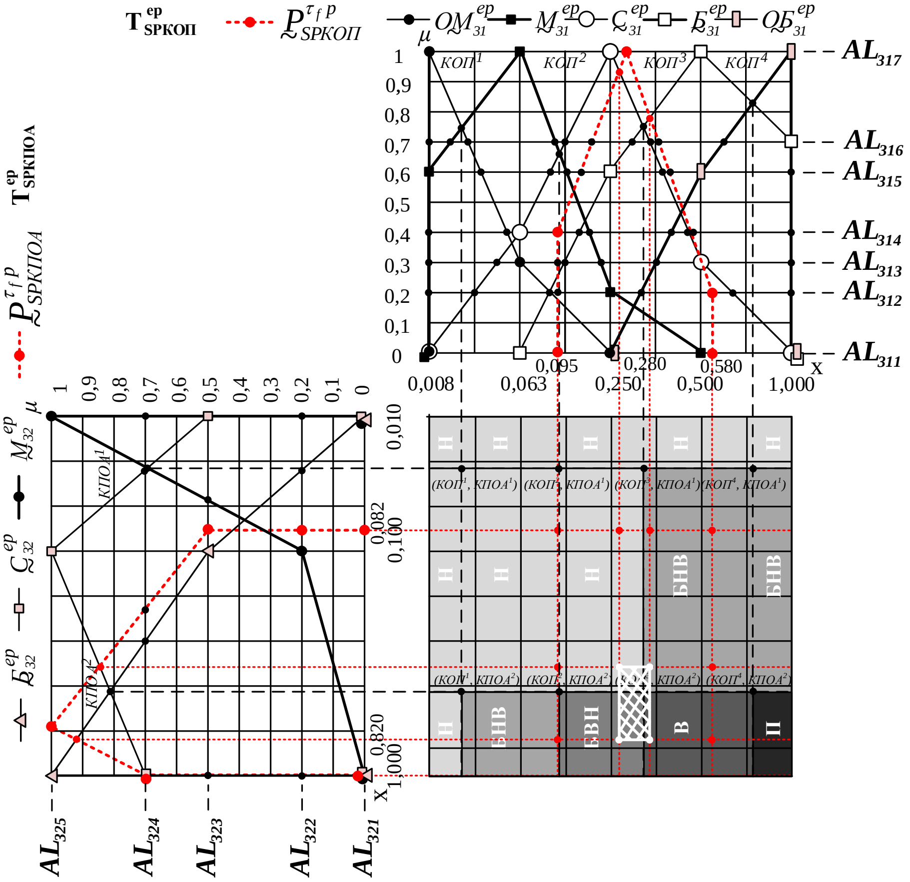

Рис. 5. Графічна інтерпретація поточного блоку відносно фазифікованих значень $\underset{\sim}{P}_{31}^{\tau_f}$ і $\underset{\sim}{P}_{32}^{\tau_f}$ з ІД «Більш високим ніж низьким», який інтерпретує аномалію у КОП-КПОА-підсередовищі, породжену SP-середовищем

Таблиця 5

Результати моделювання впливів атакуючого SP-середовища

Підмножина детекційних виразів	Задіяний ІД аномальності	Середнє значення ЕК кібератаки	Кількість кібератак	Відсоток виявлених кібератак
$\mathbf{DR}_{3\ 13}$	БВН	0,652	647	32,35%
$\mathbf{DR}_{3\ 14}$	В	0,785	910	45,5%
$\mathbf{DR}_{3\ 15}$	П	0,715	443	22,15%

Як видно з таблиці, вся множина модельованих кібератак була відповідно виявлена умовними виразами SP-середовища з ІД аномальності «Більш високий ніж низький», «Високий» та «Граничний» (П), що входять у підмножини детекційних виразів $\mathbf{DR}_{3\ 13}$, $\mathbf{DR}_{3\ 14}$ та $\mathbf{DR}_{3\ 15}$, на кожне з яких відповідно припало 32,35%, 45,5% та 22,15% реалізованих загроз на ФС.

ВИСНОВКИ

Проведені за допомогою емулятора експериментальні дослідження підтвердили достовірність основних теоретичних положень, практичних розробок та адекватність роботи програмного модуля СВК.

ЛІТЕРАТУРА

[1] Анализ и классификация методов обнаружения сетевых атак / А. А. Браницкий, А. В. Котенко // *Тр. СПИИРАН*. 2016. № 2 (45). С. 207-244.

[2] Сучасні методи виявлення аномалій в системах виявлення вторгнень / О. М. Колодчак // *Вісник Національного ун-т «Львівська політехніка». Комп'ютерні системи та мережі*. 2012. № 745. С. 98-104.

[3] A Survey and Comparative Analysis of Data Mining Techniques for Network Intrusion Detection Systems / R. Patel, A. Thakkar, A. Ganatra. India: International Journal of Soft Computing and Engineering (IJSCE), 2012. Vol. 2. Issue 1. pp.265-260 .

[4] *The State of the Art in Intrusion Prevention and Detection* [Electronic resourse] / Al-Sakib Khan Pathan. New York: Auerbach Publications, 2014. 516 p. URL: http://docshare03.docshare.tips/files/20579/205795770.pdf.

[5] Розробка моделі інтелектуального розпізнавання аномалій і кібератак з використанням логічних процедур, які базуються на покриттях матриць ознак / Г. Бекетова, Б. Ахметов, О. Корченко, В. Лахно // *Безпека інформації*. К: НАУ, 2016. Т. 22, № 3. С. 242-254.

[6] Аналіз системи виявлення вторгнень та комп'ютерних атак / М. М. Радченко [та ін.] // *Междисциплинарные исследования в науке и образовании*. 2013. № 2.

[7] Analysis of Host-Based and Network-Based Intrusion Detection System / Amrit Pal Singh, Manik Deep Singh. India: I. J. *Computer Network and Information Security*, 2014. Vol. 8. - pp.41-47.

[8] Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware / O. B. Lawal [et al.] // *African Journal of Computing & ICT. Ibadan*, 2013. Vol. 6, No. 2. pp. 169-184.

[9] *Top Intrusion Detection Tools for 2018* [Electronic resourse] / S. Cooper. Maidstone, Kent: Comparitech, 2018. URL: https://www.comparitech.com/net-admin/network-intrusion-detection-tools/.

[10] *Understanding modern intrusion detection systems: a survey* [Electronic resourse] / Liu Hua Yeo [et al.]. Michigan: Eastern Michigan University, 2017. URL: https://arxiv.org/ftp/arxiv/papers/1708/1708.07174.pdf.

[11] А. Корченко, «Кортежная модель формирования набора базовых компонент для выявления кибератак», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, В.2 (28), 2014. - С. 29-36.

[12] A. Korchenko, K. Warwas, A. Kłos-Witkowska, «The Tupel Model of Basic Components' Set Formation for Cyberattacks», in Intelligent Data Acquisition and Advanced Computing Systems: *Technology and Applications (IDAACS)*, 2015 IEEE 8th International Conference on, 2015. - pp. 478-483.

[13] B. Akhemetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva, *«Improved method for the formation of linguistic standards for of intrusion detection systems», Journal of Theoretical and Applied Information Technology*, vol. 87, no. 2, 2016. - pp. 221-232.

[14] M. Karpinski, A. Korchenko, P. Vikulov, R. Kochan, «The Etalon Models of Linguistic Variables for Sniffing-Attack Detection», in *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2017 IEEE 9th International Conference on, 2017.- pp. 258-264.

[15] А. Корченко, «Метод формирования лингвистических эталонов для систем выявления вторжений», *Захист інформації*, Т.16, №1, 2014. - С. 5-12.

[16] И. Терейковский, А. Корченко, П. Викулов, А. Шаховал, «Модели эталонов лингвистических переменных для обнаружения сниффинг-атак», *Захист інформації*, Т.19, №3, 2017. - С. 228-242.

[17] І. Терейковський, А. Корченко, П. Вікулов, І. Ірейфідж, «Моделі еталонів лінгвістичних змінних для систем виявлення email-спуфінг-атак», Безпека інформації, Т.24, №2, 2018. - С. 99-109.

[18] А. Корченко, «Метод фаззификации параметров лингвистических эталонах для систем выявления кибератак», *Безпека інформації*, Т.20, №1, 2014. - С. 21-28.

[19] А. Корченко, «Метод α-уровневой номинализа-

ции нечетких чисел для систем обнаружения вторжений», *Захист інформації*, Т.16, №4, 2014. - С. 292-304.

[20] А. Корченко, «Метод определения идентифицирующих термов для систем обнаружения вторжений», *Безпека інформації*, Т.20, №3, 2014. - С. 217-223.

[21] Н. Карпинский, А. Корченко, С. Ахметова, «Метод формирования базовых детекционных правил для систем обнаружения», *Захист інформації*, Т.17, №4, 2015. - С. 312-324.

[22] А. Корченко, В. Щербина, Н. Вишневская, «Методология построения систем выявления аномалий, порожденных кибератаками», *Захист інформації*, Т.18, №1, 2016. - С. 30-38.

[23] И. Терейковский, А. Корченко, «Система выявления кибератак», *Безпека інформації*, Т.23, №3, 2017. - С. 176-180.

[24] ПЗ А. Корченко, О. Заріцький, Т. Паращук, В. Бичков, «Програмне забезпечення формування еталонів параметрів для систем виявлення кібератак», *Захист інформації*, Т.20, №3, 2018. - С. 133-148.

[25] А. Корченко *Методи ідентифікації аномальних станів для систем виявлення вторгнень.* Монографія, Київ, ЦП «Компринт», 2019. – 361 с.

[26] *Обзор мирового и российского рынков средств симуляции кибератак (Breach and Attack Simulation, BAS) 2021* [Электронный ресурс] // URL: https://www.anti-malware.ru/analytics/Market_Analysis/Breach-and-Attack-Simulation-Market-Overview.

[27] *Генерация трафика web-приложений и кибератак* [Электронный ресурс] // URL: https://spirent.pr-group.ru/generatory-trafika-spirent/generaciya-trafica-prilozheniy-i-cyberatak/.

[28] *Microsoft представила симулятор кибератак с машинным обучением* [Электронный ресурс] // URL: https://habr.com/ru/news/t/551558/.

[29] *Програмний модуль формування еталонів параметрів для систем виявлення аномалій. Комп'ютерна програма* / Т. Паращук, А. Корченко – К. – Свідоцтво про реєстрацію авторського права на твір №74016 від 02.10.2017.

[30] А.О. Корченко, Є.В. Іванченко, В.В. Погорелов, «Оцінювання ефективності експертної системи виявлення вторгнень на базі нечіткої логіки», *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки*, Т.30 (69), №1, 2019. - С. 66-72.

ЭМУЛЯТОР УГРОЗ ДЛЯ ВЕРИФИКАЦИИ СИСТЕМ ОБНАРУЖЕНИЯ КИБЕРАТАК

На сегодня, одними из распространенных систем защиты информации являются системы обнаружения кибератак и системы обнаружения вторжений, последние из которых представляют особый практический и научный интерес. Также, функциональность современных систем обнаружения и блокирования вторжений в значительной степени зависит от их возможностей по выявлению новых кибератак в режиме реального времени. Для выявления соответствующих атакующих действий используются специальные методы, модели, средства, программное обеспечение и комплексные технические решения для систем обнаружения вторжений, которые могут оставаться эффективными при появлении новых или модифицированных киберугроз. Однако, как показывает практика при появлении новых угроз и аномалий, порожденных атакующими действиями с неустановленными или нечетко определенными свойствами, соответствующие средства не всегда остаются эффективными. Таким образом, разработка средств верификации и проведения экспериментальных исследований соответствующих технических решений, программного обеспечения обнаружения кибератак, злоупотреблений и аномалий в информационных системах для подтверждения адекватности их работы является актуальной научной задачей. Есть ряд работ, таких как кортежных модель формирования атакующих сред, ряд методов для выявления аномальных состояний, методология построения системы обнаружения вторжений, а также структурная модель вычислительной системы для создания средств обнаружения кибератак и ее алгоритмическое и программное обеспечение. Для ее верификации необходим специализированный эмулятор киберугроз, поскольку известные не поддерживают необходимые форматы данных, применяемых в авторской разработке. Исходя из этого, целью работы является разработка эмулятора для проведения экспериментального исследования для подтверждения достоверности полученных теоретических положений, практических результатов и адекватности работы программного модуля разработанной системы обнаружения кибератак, что позволит усовершенствовать функциональные свойства современных систем обнаружения вторжений для режима реального времени.

Ключевые слова: атаки, кибератаки, аномалии, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак, системы обнаружения кибератак, выявление аномалий в компьютерных сетях.

THREAT EMULATOR FOR VERIFICATION OF CYBERATIC DETECTION SYSTEMS

Today, one of the most common information security systems is cyberattack detection and intrusion detection systems, the second have a particular practical and scientific interest. Also, the functionality of modern intrusion detection and blocking systems largely depends on their ability to detect new cyberattacks in real time. Special methods, models, tools, software and comprehensive technical solutions for intrusion detection systems are used to detect appropriate attacks, which are effective with new or modified cyber threats. However, in practice when new threats and anomalies generated by attacking the actions of unidentified or poorly properties,

appropriate means are not always effective. Therefore, the development of verification tools and experimental research of relevant technical solutions, tools and software to detect cyberattacks, abuses and anomalies in information systems to confirm the adequacy of their work is an urgent scientific task. There are a number of works, such as a tuple model of attack environments, a number of methods for detecting anomalous states, a methodology for building an intrusion detection system, and a structural model of a computer system to create cyberattacks and its algorithmic and software. To verify it, a specialized cyber threat emulator is needed, as the known ones do not support the necessary data formats used in the author's development. Based on this, the aim is to develop an emulator for experimental research to confirm the reliability of the obtained theoretical provisions, practical results and adequacy of the software module of the developed cyberattack detection system, which will improve the functional properties of modern intrusion detection systems for real time.

Keywords: attacks, cyberattacks, anomalies, intrusion detection systems, anomaly detection systems, attack detection systems, cyberattack detection systems, anomaly detection in computer networks.

Корченко Анна Олександрівна, доктор технічних наук, доцент, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: annakor@ukr.net.
Orcid ID: 0000-0003-0016-1966.
Корченко Анна Александровна, доктор технических наук, доцент, профессор кафедры безопасности информационных технологий Национального авиационного университета.
Korchenko Anna, Dr Eng (Information security), Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

Дрейс Юрій Олександрович, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету, старший науковий співробітник Національної академії СБ України.
E-mail: y.dreis@nau.edu.ua.
Orcid ID: 0000-0003-2699-1597.
Дрейс Юрий Александрович, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета, старший научный сотрудник Национальной академии СБ Украины.
Yurii Dreis, PhD Eng (Information Security), Associate Professor of IT-Security Academic Department, National Aviation University, Senior Researcher of Scientific Department, National Academy of Security Service of Ukraine.

Нагорний Юрій Іванович, кандидат технічних наук, викладач спеціальних дисциплін відокремленого структурного підрозділу «Новокаховський фаховий коледж Таврійського державного агротехнологічного університету імені Дмитра Моторного».
E-mail: ur.duran@gmail.com.
Orcid ID: 0000-0002-6437-3629.
Нагорный Юрий Иванович, кандидат технических наук, преподаватель специальных дисциплин обособленного структурного подразделения «Новокаховский профессиональный колледж Таврийского государственного агротехнологического университета имени Дмитрия Моторного».
Yurii Nahornyi, candidate of technical sciences, teacher of special disciplines of a separate structural subdivision «Novokakhovka vocational college of the Tavriya state agrotechnological university named after Dmitry Motorny».

Бичков Володимир Вячеславович, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету.
Email: bychkov.volodymyr@gmail.com.
Orcid ID: 0000-0002-1054-9182.
Бичков Владимир Вячеславович, старший преподаватель кафедры безопасности информационных технологий Национального авиационного университета.
Volodymyr Bychkov, Senior Lecturer of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

DOI: 10.18372/2410-7840.23.15728
УДК 004.056.53

МОДЕЛЬ НЕЧІТКОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ НА ОСНОВІ ПОВЕДІНКОВОЇ БІОМЕТРІЇ

Віталій Фесьоха, Надія Фесьоха

У статті розглянуто актуальне наукове завдання кіберзахисту інформаційних систем органів військового управління від несанкціонованого доступу. Запропоновано модель автентифікації користувачів інформаційних систем, яка ґрунтується на використанні поведінкової біометрії та математичного апарату теорії нечіткої логіки. Суть запропоно-