ISSN 2219-9365

УДК 519.857.3
DOI: 10.31891/2219-9365-2021-68-2-3

ДЬОГТЄВА І. О., ШИЯН А. А.
Вінницький національний технічний університет

ВІДНОВЛЕННЯ ГРУПИ РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ НАРОСТАННЯ ІНТЕНСИВНОСТІ КІБЕРАТАК

Метою статті є розробка моделі для опису функціонування групи реагування на інциденти інформаційної безпеки (ГРІІБ) в умовах урахування як наростання інтенсивності кібератак, так і відновлення її роботи в процесі діяльності. Для опису роботи ГРІІБ застосовується модель системи масового обслуговування в рамках марковського процесу, де кібератаки представлені потоком заявок, а група реагування розглядається в якості каналу їх обслуговування. Отримано кількісні результати для динаміки кількості обслужених (коли протидія кібератакам була здійснена) та втрачених (коли протидія не могла бути здійснена) заявок. Показано, що відповідні характеристики нелінійно залежать від характеристик моделі: інтенсивності кібератак, їх наростання та характеристик відновлення ефективної діяльності ГРІІБ. Розроблена модель може бути використана для оптимізації управління функціонування ГРІІБ в залежності від характеристик кібератак та відновлення діяльності групи реагування. Вона також надає можливість керівникам орієнтуватися на потрібну кількість реагувань чи відмов у реагуванні на інциденти інформаційної безпеки.

Ключові слова: кібератака, група реагування на інциденти інформаційної безпеки, система масового обслуговування, марковський процес, функція розподілу, функція відновлення.

I. DOHTIEVA, A. SHYIAN
Vinnytsia National Technical University

RECOVERY OF THE INFORMATION SECURITY INCIDENT RESPONSE TEAM IN THE CONTEXT OF INCREASING CYBER ATTACKS

The purpose of the article is to develop a model to describe the functioning of information security incident response teams (ISIRT) in terms of increasing the intensity of cyber attacks, and the resumption of its work in the process. The queuing system model is used to describe the work of ISIRT within the Markov process, where cyber attacks are represented by a stream of requests at random times, and the response team is considered as a channel for their service. The process of restoring the effective work of ISIRT is also random, as it depends on many random characteristics (for example, the specifics of communication in the group, access to relevant information, etc.).

The article obtained quantitative results for the dynamics of the number of served (when countering cyber attacks) and lost (when countering could not be carried out) applications. It is shown that the corresponding characteristics nonlinearly depend on the characteristics of the model: the intensity of cyber attacks, their increase and the characteristics of the restoration of effective ISIRT.

The proposed model proposes to carry out two-factor optimization of ISIRT operation in real time. Optimization can be carried out on the effectiveness of the ISIRT in relation to the maximum effectiveness of serviced or lost responses to cyber attacks or its elements. This allows you to respond quickly to changes in the specifics of cyber attacks (or a set of cyber attacks), and the requirements of management on the need for increased attention to serviced or lost cyber attacks or their elements. The developed model can be used to optimize the management of ISIRT depending on the characteristics of cyber attacks and the resumption of the response team.

Keywords: cyber attack, information security incident response team, queuing system, Markov process, distribution function, recovery function.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Останнім часом стрімко зростає використання кіберпростору для дестабілізації соціального стану суспільства [1]. Все частіше певні соціальні групи стають мішенню для здійснення на них негативного інформаційно-психологічного впливу, формування у них намірів здійснювати шкідливу для суспільства поведінку тощо. Якщо раніше цільовими точками кібератак ставала переважно технічна компонента соціотехнічних систем, то сьогодні кіберзлочинці тримають в полі зору соціальну компоненту таких систем [2].

Наведені тенденції породжують нові вимоги до функціонування груп реагування на інциденти інформації безпеки (ГРІІБ). Тепер повинні створюватися такі ГРІІБ, завданням яких є реагування на кібератаки, ціллю яких є дестабілізація соціальних груп чи навіть суспільства у цілому [3]. Спеціалісти, які працюють в таких групах, повинні вміти ідентифікувати елементи кібератаки, які створюють негативний вплив на соціальні спільноти (наприклад, фейки, недостовірну, неповну чи перекручену інформацію тощо) [4]. Поряд з цим спеціалісти ГРІІБ повинні також розробляти комплекс протидії таким інцидентам, враховуючи специфічні особливості як функціонування кіберпростору, так і сприйняття інформації заданими спільнотами [5]. Нарешті ГРІІБ повинна запропонувати комплекс заходів, які спроможні ліквідувати негативні наслідки у зацікавлених спільнотах, формуючи інформаційні пакети в потрібному для досягнення найбільшого ефекту вигляді.

Аналіз досліджень та публікацій

Необхідність саме такого режиму в діяльності ГРІБ переконливо довели вибори в США в 2016 році. Зокрема, в [6] зроблено такий висновок (переклад авторів): «Спираючись на дані веб-перегляду, архіви веб-сайтів для перевірки фактів та результати нового онлайн-опитування, ми виявили: 1) соціальні медіа були важливим, але не домінуючим джерелом новин про вибори: 14% американців називали соціальні медіа своїм «найбільш важливим» джерелом; 2) з відомих неправдивих новин, які з'явилися за три місяці до виборів, прихильники Трампа у Facebook ними поділилися загалом 30 мільйонів разів, а прихильники Клінтон – 8 мільйонів разів; 3) середньостатистичний дорослий американець бачив приблизно одну або, можливо, кілька фейкових новин протягом виборчої кампанії, причому понад половина тих, хто згадав, що бачив, повірили їм; і 4) люди з більшою ймовірністю вірять історіям, які надають перевагу їхньому кандидату, особливо якщо вони мають ідеологічно відокремлені соціальні мережі.» Таким чином виявлено, що фейки та дезінформація в кіберпросторі можуть істотно впливати на прийняття рішення в окремих соціальних групах та у суспільстві в цілому. Внаслідок цього і боротьба з ними стає все більш важливою задачею для ГРІБ.

Враховуючи описане, варто також підкреслити, що тривалість такої боротьби буде зростати, оскільки саме розгортання атаки може тривати від декількох днів до декількох місяців [7]. При цьому спеціалісти ГРІБ повинні весь цей час підтримувати дуже напружений режим роботи в умовах високого рівня стресу [8]. З часом розгортання як окремої кібератаки, так і серії кібератак, рівні напруження та стресу тільки зростають. Таким чином, виникає необхідність у відновленні працездатності як окремих спеціалістів, так і ГРІБ у цілому, так як із часом в таких умовах збільшується ймовірність можливості допущення помилок [9, 10]. Варто підкреслити, що раніше задача про відновлення роботи ГРІБ в процесі протидії кібератакам не стояла так гостро внаслідок того, що такі атаки тривали відносно невеликий час.

Виділення невирішених раніше частин загальної проблеми

Оскільки кібератаки розпочинаються у випадковий проміжок часу, то вони можуть моделюватися з використанням марковських процесів [10]. Варто зазначити, що і процес відновлення ефективної роботи ГРІБ також носить випадковий характер, так як він залежить від багатьох випадкових характеристик. Наприклад, від індивідуальних особливостей спеціаліста, від специфіки комунікації в групі, від доступу до потрібної інформації та до експертів тощо.

З точки зору моделювання, функціонування ГРІБ можна представити як діяльність системи масового обслуговування (СМО). Роль потоку заявок тут відіграють кібератаки, а в якості каналу обслуговування – сама ГРІБ. Найбільш привабливими випадковими процесами, що описують функціонування систем обслуговування є марковські процеси, математичний апарат такого дослідження дозволяє отримати аналітичні вирази для показників якості [10].

Формулювання цілей статті

Формулювання цілі статті. Метою дослідження є розробка моделі для опису функціонування ГРІБ в умовах урахування як наростання інтенсивності кібератак, так і відновлення її роботи в процесі діяльності.

Виклад основного матеріалу

Алгоритмічний опис моделі для функціонування ГРІБ під час кібератаки. Враховуючи випадковість у виникненні подій інформаційної безпеки, функціонування ГРІБ пропонується моделювати на базі марковських процесів на прикладі системи масового обслуговування (СМО), специфічність якої полягає в наявності параметру підвищення інтенсивності ідентифікації подій інформаційної безпеки.

Нехай розгортання в часі кібератаки представлене у вигляді рекурентного потоку заявок (інцидентів) на реагування, який описується розподілом:

$$F(t)=\begin{cases}0, & t<0,\\ 1-e^{\alpha\lambda t}, & t\geq 0,\end{cases} \tag{1}$$

де $\alpha\lambda$ – параметр інтенсивності, $\alpha>0$ – кількісна характеристика зростання насиченості кібератаки (збільшення швидкості, об'єму та складності кібертатаки, розширення площі атак, мультивекторний підхід в атаках тощо). Тривалість обробки інцидентів ГРІБ задається показниковим законом розподілу, який має параметр μ:

$$G(t)=\begin{cases}0, & t<0,\\ 1-e^{\mu t}, & t\geq 0.\end{cases} \tag{2}$$

Для опису діяльності ГРІІБ вибрана модель M/M/1/0 з підвищенням інтенсивності надходження заявки за умови незайнятості. Процес діяльності ГРІІБ можна описати марковським процесом $\xi(t)$, який характеризується множиною станів $\{e_0, e_1\}$.

Перехідний процес обслуговування у даній системі масового обслуговування у випадку збільшення робочого навантаження здійснюється згідно з вкладеним ланцюгом Маркова [11], який задається матрицею перехідних ймовірностей відповідно до (1) та (2):

$$P = \begin{pmatrix} 0 & 1 \\ \frac{\mu}{\lambda+\mu} & \frac{\lambda}{\lambda+\mu} \end{pmatrix} \tag{3}$$

Вихідними даними для моделювання є інтенсивність потоку заявок λ (інтенсивність надходження заявок), параметр навантаження α (параметр підвищення інтенсивності надходження заявок), продуктивність каналу (сервера) μ обслуговування заявок (інтенсивність обслуговування заявок)), кількість реалізацій N^* (кількість циклів для проведення сценаріїв експериментів), що забезпечують задану точність розрахунку, та в загальному випадку границя інтервалу часу T.

Процес функціонування системи може розглядатись за період часу $[0; T]$. Даний період в своїх граничних межах накладає обмеження: заявки, для яких момент появи $t_i \geq T$, де t_i – черговий момент надходження заявки, в систему не потрапляють і не обслуговуються; заявки, для яких час завершення обслуговування перевищують граничні межі часового проміжку, вважаються такими, які отримали відмову.

В якості початкових умов для моделювання обрано відповідні значення: $i = \overline{1, n}$, $t_0 = 0$, $t_0^{(se)} = \eta_0^{\mu}$, $N = 0$, $N^{(l)} = 0$, $N^{(s)} = 0$.

Загалом алгоритм для процесу функціонування одноканальної СМО може бути представлений в операторній формі [12]. Для випадку запропонованої моделі ГРІІБ така форма має вигляд:

$$\begin{array}{ccccc} {}^{9,11,13}G_1, & F_2, & C_{3\downarrow 12}, & C_{4\downarrow 10}, & F_5, \\ F_6, & C_{7\downarrow 11}, & CAL_8, & CAL_9{}^1, & {}^4F_{10}, \\ {}^7CAL_{11}{}^1, & {}^3CAL_{12}, & C_{13\downarrow 1}, & CAL_{14}, & F_{15}. \end{array} \tag{4}$$

На рис. 1 подано алгоритмічну схему процесу функціонування роботи ГРІІБ в межах операторної форми (4).

Оператор G_1 відповідає за формування: $\tau_i^{\alpha\lambda}$ – показниково розподілена випадкова величина (1) з параметром $\alpha\lambda$ (інтервали часу між надходженнями заявок з підвищеною інтесивністю); τ_i^{λ} – показниково розподілена випадкова величина з параметром λ (інтервали часу між надходженнями заявок в нормальному режимі); η_i^{μ} – показниково розподілена випадкова величина (2) з параметром μ (час обслуговування). Далі управління передається оператору F_2, який формує момент надходження заявки t_i:

$$t_i = \begin{cases} t_{i-1} + \tau_{i-1}^{\alpha\lambda}, t_{i-1} + \tau_{i-1}^{\lambda} \geq t_{i-1}^{(se)} \\ t_{i-1} + \tau_{i-1}^{\lambda}, t_{i-1} + \tau_{i-1}^{\lambda} < t_{i-1}^{(se)} \end{cases} \tag{5}$$

Оператор C_3 перевіряє, чи належить дана заявка інтервалу часу $[0; T]$. Якщо $t_i \geq T$, то t_i не належить періоду часу моделювання (реалізація завершилась), управління передається оператору CAL_{12} для підрахунку кількості реалізацій ($N+1$). Після збору даної статистики, оператор C_{13} перевіряє на предмет необхідної кількість реалізацій $N < N^*$. Якщо дана кількість недостатня, то управління передається оператору G_1, який здійснює перехід до чергової реалізації. Якщо (реалізацій достатньо) $N = N^*$ –

управління передається оператору для обробки результатів моделювання CAL_{14}, та експеримент завершується F_{15}. Якщо умову $t_i < T$, що перевіряється оператором C_3, виконано – заявка належить даній реалізації; тоді керування передається оператору C_4. Даний оператор за допомогою перевірки нерівності $t_i \geq t_{i-1}^{(se)}$ визначає, вільний чи зайнятий канал обслуговування.

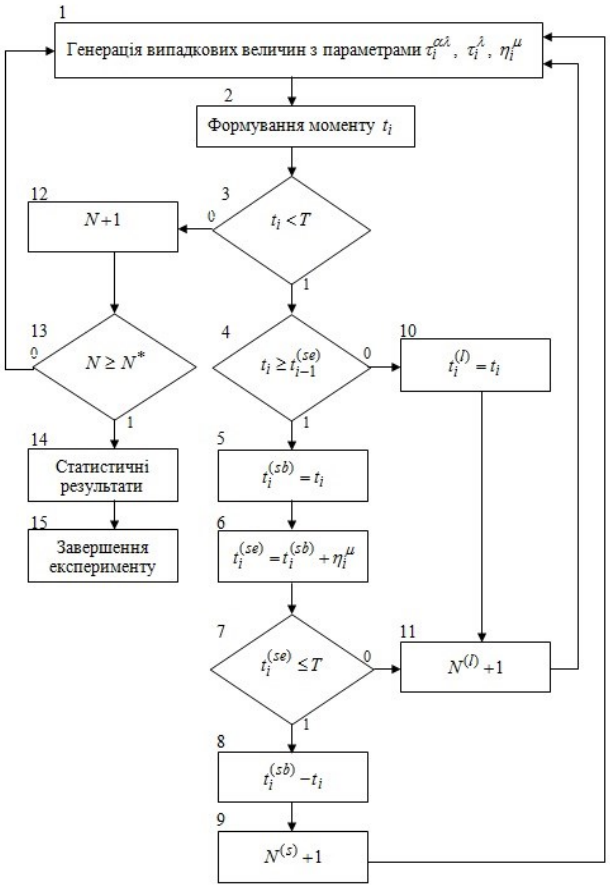


Рис. 1. Алгоритмічна схема діяльності ГРІБ в умовах навантаження інцидентами

Якщо канал зайнятий обслуговуванням попередньої заявки, $t_i < t_{i-1}^{(se)}$, то управління передається оператору F_{10}, який фіксує момент відмови $t_i^{(l)}$. Далі процес передається оператору CAL_{11}, який підраховує число заявок, які отримали відмову ($N^{(l)}+1$), і передає управління оператору генерації F_1, який після реалізації генерації формує нове t_i (5) в межах оператора F_2.

Якщо $t_i \geq t_{i-1}^{(se)}$ (канал вільний), то управління передається оператору F_5, який формує $t_i^{(sb)}$ – момент початку обслуговування i-ої заявки. Після чого управління передається оператору F_6, який обчислює $t_i^{(se)}$ – момент завершення обслуговування – і передає управління оператору C_7 для перевірки нерівності $t_i^{(se)} \leq T$. Якщо дана нерівність виконується, тобто момент завершення обслуговування належить даній реалізації, управління передається оператору CAL_8 для обчислення – часу очікування заявки до початку обслуговування ($t_i^{(sb)} - t_i$), а потім оператору CAL_9 для підрахунку кількості обслужених заявок ($N^{(s)}+1$). Якщо нерівність $t_i^{(se)} \leq T$ не виконується, тобто момент завершення обслуговування знаходиться поза межами даної реалізації, управління передається оператору CAL_{11}, який враховує випадки відмови.

Аналітичні вирази для функцій відновлення ГРІБ під час кібератаки. Відомо, що функція відновлення визначається як математичне очікування числа відновлень (попадань марковського процесу у певний стан), що відбулися до певного моменту t [13]. У випадку моделі ГРІБ для числа вимог: які надходять за час t ($v(t)$), які були обслужені ($v_S(t)$), та, які були втрачені за час t $v_l(t)$, маємо:

$$H_S(t)+H_l(t)=M(v_S(t))+M(v_l(t))=M(v_S(t)+v_l(t))=Mv(t)=H(t), \tag{6}$$

де $H(t)$, $H_S(t)$, $H_l(t)$ - функції відновлення пуассонівського потоку з параметром $\alpha\lambda$, потоку обслужених і потоку втрачених вимог відповідно.

Функція відновлення пуассонівського потоку з параметром $\alpha\lambda$ для системи з навантаженням для моделювання функціонування ГРІБ в умовах наростання інтенсивності кібератак дорівнює:

$$H(t)=\alpha\lambda t \tag{7}$$

В рамках знаходження функції відновлення потоку обслужених вимог використано опис аналізу поведінки системи на проміжку часу $(t+\Delta t)$, де відповідно до формули повної ймовірності отримано ряд рівностей для $n=1,2,...$ на базі ймовірностей $P_{n0}(t)$ та $P_{n1}(t)$, того, що процес $\xi(t)$ в момент часу t знаходиться відповідно у станах e_0 (система вільна) та e_1 (система зайнята) і за цей час обслужено n вимог. В результаті диференційованості функцій $\overline{P}_{n0}$ та $\overline{P}_{n1}$ ($n=1,2,...$), отримано нескінченну систему диференціальних рівнянь. Використання твірних функцій для послідовностей $(\overline{P}_{n0}(t))$ та $(\overline{P}_{n1}(t))$ дозволило отримати лінійні рівняння другого порядку із сталими коефіцієнтами та відповідно розв'язки характеристичного рівняння для даних рівнянь. Далі, отримавши запис твірної функції послідовності $(\overline{P}_n(t))$ та врахувавши, що $H_S(t)=M(v_S(t))$, в результаті перетворень знайдено математичне вираження функції відновлення потоку обслужених вимог для моделі ГРІБ, яка моделюється системою масового обслуговування M/M/1/0 з підвищенням інтенсивності надходження вимоги за умови незайнятості системи:

$$H_S(t)=\frac{\alpha\lambda(\lambda+\mu)}{(\alpha+1)\lambda+\mu}t-\frac{\alpha\lambda(\lambda+\mu)}{((\alpha+1)\lambda+\mu)^2}\left(1-e^{-((\alpha+1)\lambda+\mu)t}\right) \tag{8}$$

Враховуючи (7), (8) та умову (6) маємо аналітичний вираз для функції відновлення потоку втрачених вимог:

$$H_l(t)=\frac{\alpha^2\lambda^2}{(\alpha+1)\lambda+\mu}t+\frac{\alpha\lambda(\lambda+\mu)}{((\alpha+1)\lambda+\mu)^2}\left(1-e^{-((\alpha+1)\lambda+\mu)t}\right) \tag{9}$$

Імітаційне моделювання. Для розробки даної реалізації було обрано мову програмування Python, яка застосовується для рішень широкого спектру задач, зокрема, для роботи з даними в наукових дослідженнях, Data Mining, Data Science, тощо. Використано ряд бібліотечних та сторонніх модулів, серед яких: пакети NumPy, Pandas, бібліотека Matplotlib зі стеку SciPy; Statsmodels, тощо [14]. Для побудови тривимірних графіків (3D графіка) в динаміці використано mplot3d Toolkit з пакету Matplotlib [15].

На рис. 2 подано приклад вхідних даних, використанні при моделюванні.

```
Output data:
Intensity of the receipt of requests                              : 1.5
The parameter to increase the intensity of the receipt of requests  : 2
Intensity of service of requests                                  : 3.5
Number of cycles for each experiment                              : 100
```

Рис. 2. Вхідні дані M/M/1/0 (модель ГРІБ) з підвищенням інтенсивності надходження заявки за умови незайнятості системи

В імітаційному середовищі пропонується моделювати поведінку функцій відновлення роботи системи з навантаженням в двовимірному та тривимірному просторах.

Рис. 3 демонструє поведінку функцій відновлення (7), (8), (9) на площині, де визначена залежність даних функцій від безпосередньо часової характеристики, визначеного періоду моделювання (процес відновлення в умовах розгортання кібератаки в часі). Варто зазначити, що у випадку (8), (9) графіки представлені прямими,адже їх залишкова показникова частина, при збільшенні значення t втрачає свій вплив на поведінку функцій.

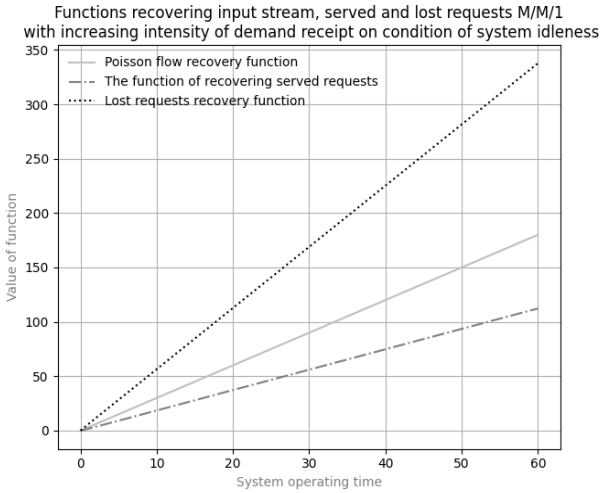


Рис. 3. Графіки функцій відновлення вхідного потоку, обслужених та втрачених вимог M/M/1/0 з підвищенням інтенсивності надходження вимоги за умови незайнятості системи

Представлення графіків в трьох просторових вимірах дозволяє моделювати поведінку функцій відновлення потоку обслужених та втрачених вимог з залученням більшої кількості динамічних змінних, зокрема враховувати вплив вхідних параметрів функціонування досліджуваної системи: α - параметр навантаження (параметр підвищення інтенсивності надходження заявок); λ - інтенсивність потоку заявок (інтенсивність надходження заявок); μ - продуктивність каналу (сервера) обслуговування заявок (інтенсивність обслуговування заявок).

По суті функції відновлення пропонується розглянути в якості функцій двох змінних. Для функції відновлення обслужених вимог (8) розглянуті варіанти: $H_S(\alpha,t)$, $H_S(\lambda,t)$, $H_S(\mu,t)$, для функції відновлення втрачених вимог (9) - $H_l(\alpha,t)$, $H_l(\lambda,t)$, $H_l(\mu,t)$.

На рис. 4 подано розраховані графіки для варіантів числових значень функцій відновлення обслужених $H_S(\alpha,t)$ та втрачених $H_l(\alpha,t)$ вимог в залежності від параметру навантаження α та часу t в процесі кібератаки. На рисунку для порівняння показано значення функцій відновлення $H_S(t)$ (8) та $H_l(t)$ (9) відповідно, які не залежить від параметру навантаження α.

На рис 5 продемонстровані перерізи (8) та (9) відповідно з графіками функцій відновлення обслужених $H_S(\lambda,t)$ та втрачених $H_l(\lambda,t)$ вимог, де врахована залежність від інтенсивності надходження заявок λ та часу t в процесі кібератаки, але в умовах навантаження.

Рис. 6 дозволяє аналізувати графіки функцій відновлення обслужених $H_S(\mu,t)$ та втрачених $H_l(\mu,t)$ вимог в залежності від інтенсивності обслуговування заявок μ та часу t в процесі кібератаки, в порівнянні з даними графіків функцій (8) та (9), які не залежить від параметру μ.

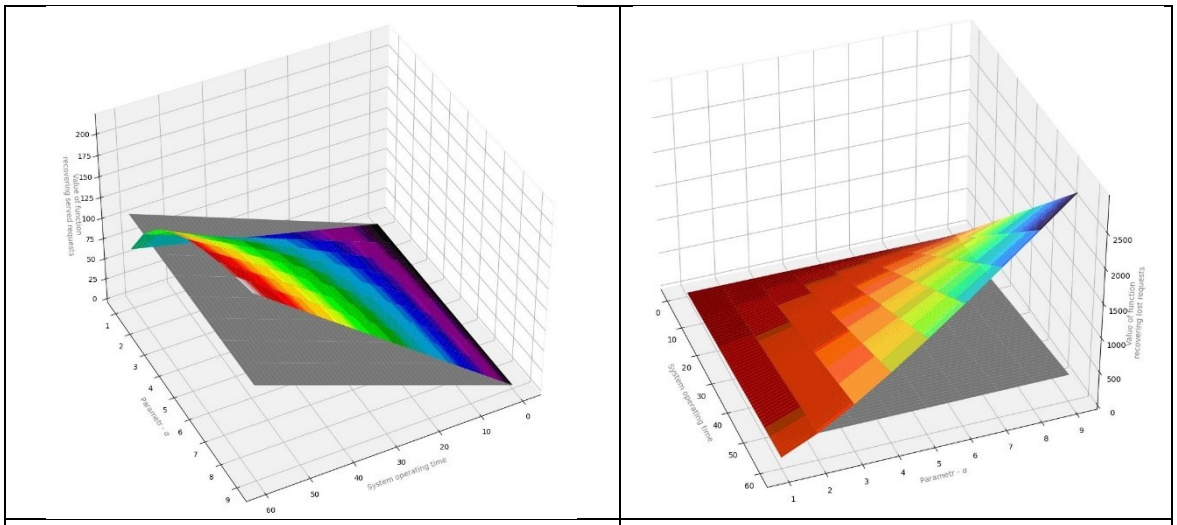
Обговорення результатів та перспективи подальшого розвитку досліджень. Отримані результати показують, що як врахування інтенсивності кібератак, так і характеристики відновлення можуть серйозно впливати на функціонування ГРІБ. Виявлено, що цей вплив є нелінійним, а відхилення від певних усереднених величин можуть бути досить значними. Про це свідчать рис. 4-6.

ГРІБ відрізняються одна від одної як кількісним складом спеціалістів, так і показниками, які характеризують як окремих спеціалістів групи, так і саму групу в цілому. Наприклад, це можуть бути такі показники [7-9]: стресостійкість спеціаліста, час утримання ним уваги, здатність ефективно працювати в несприятливих умовах (включаючи втому), час та умови для відновлення працездатності, ефективність комунікації спеціалістів при командній роботі тощо. В результаті можна розподілити ГРІБ за такими комплексними характеристиками, які можуть бути охарактеризовані такими показниками запропонованої моделі, які відповідають як за ефективність роботи групи, так і за відновлення ефективної спільної роботи всієї групи.

До того ж, можна розглядати ГРІБ із різним персональним складом спеціалістів (кількісним та якісним – в сенсі показників запропонованої моделі), що дозволить сформувати базу даних за показником μ

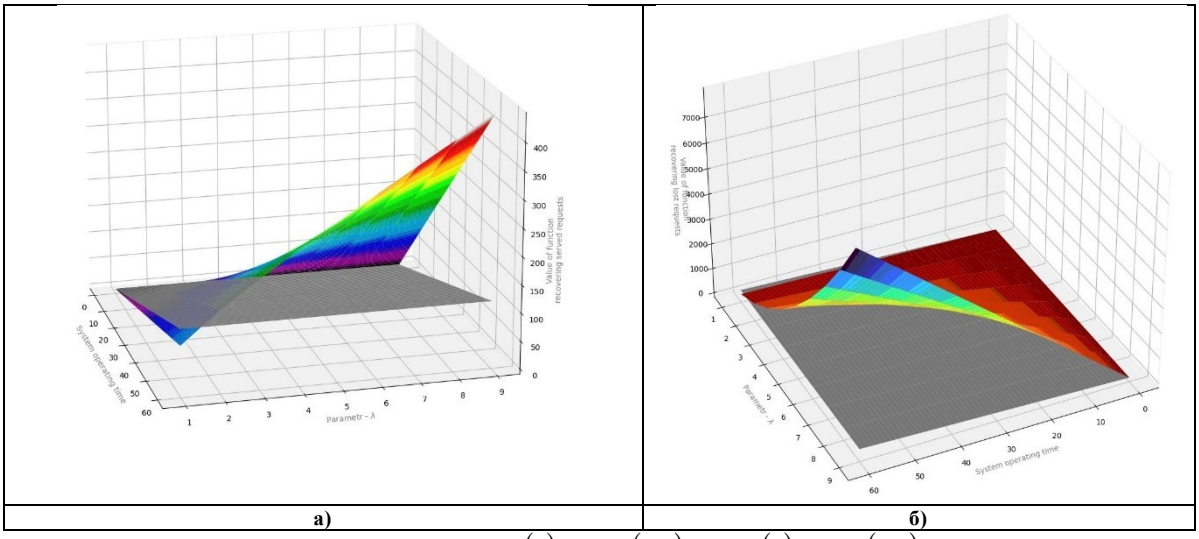
.

ISSN 2219-9365



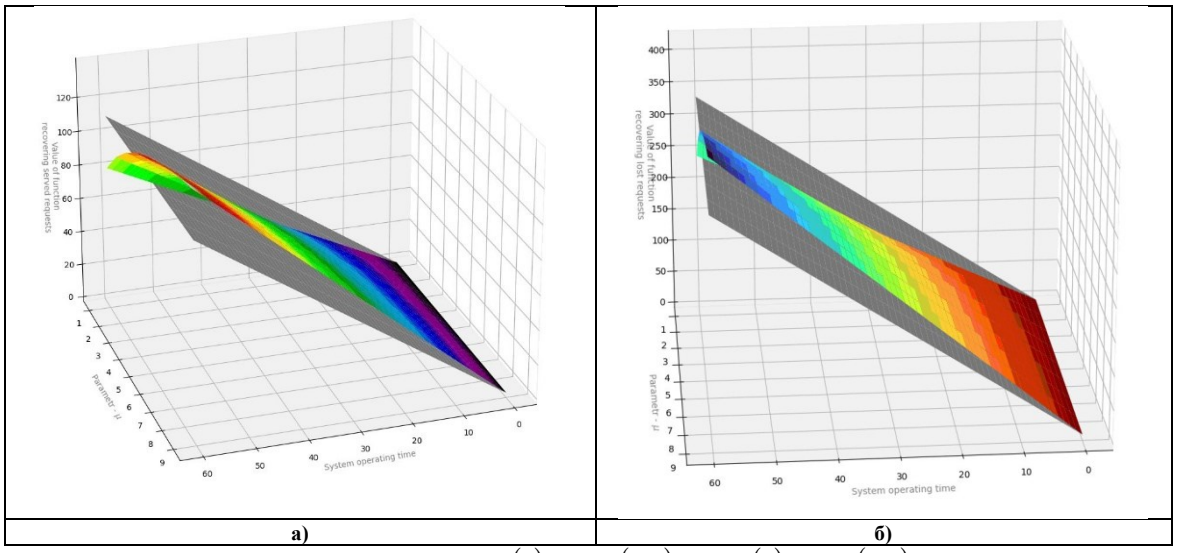
а) **б)**

Рис.4. Графіки перерізів $H_S(t)$ **та** $H_S(\alpha,t)$ **(а)** $H_l(t)$ **та** $H_l(\alpha,t)$ **(б).**



а) **б)**

Рис.5. Графіки перерізів $H_S(t)$ **та** $H_S(\lambda,t)$ **(а)** $H_l(t)$ **та** $H_l(\lambda,t)$ **(б).**



а) **б)**

Рис.6. Графіки перерізів $H_S(t)$ **та** $H_S(\mu,t)$ **(а)** $H_l(t)$ **та** $H_l(\mu,t)$ **(б).**

Аналогічно можна здійснити класифікацію кібератак за характеристиками їх інтенсивності (показник λ запропонованої моделі) та показником наростання інтенсивності (показник α запропонованої моделі). Таким чином буде сформована база даних можливих кібератак.

Запропонована модель відкриває можливість, враховуючи, описані вище, бази даних (одна характеризує ГРІБ, друга – кібератаки), оптимізувати стратегію реагування на інциденти інформаційної безпеки.

Важливою також є та обставина, що таку оптимізацію можна здійснювати навіть в процесі розгортання кібератак. Наприклад, змінюючи персональний склад спеціалістів ГРІБ, замінюючи одну ГРІБ на іншу, або ж роблячи одночасно і те, і інше. Це уможливлює підвищити надійність реагування на інциденти інформаційної безпеки та захисту кіберпростору в цілому.

По суті, запропонована модель пропонує здійснювати двофакторну (за параметрами λ та μ) оптимізацію функціонування ГРІБ в режимі реального часу. Оптимізація при цьому може здійснюватися за ефективністю функціонування ГРІБ щодо максимальної ефективності обслужених або втрачених реагувань на кібератаку чи її елементи. Це дозволяє оперативно реагувати як на зміни специфіки кібератаки (чи сукупності кібератак), так і на вимоги керівництва щодо необхідності посиленої уваги до обслужених чи втрачених кібератак чи їх елементів.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Серед тенденцій сучасних кібератак в кіберпросторі виділяють динаміку в інтенсивності та досить тривалий час розгортання атаки. В таких умовах виникає необхідність відновлення ефективного функціонування ГРІБ.

В статті побудована модель для опису функціонування ГРІБ в умовах урахування як наростання інтенсивності кібератак, так і відновлення її роботи в процесі діяльності. Діяльність ГРІБ представлено функціонуванням системи масового обслуговування (СМО), де роль потоку заявок відіграють кібератаки (або окремі елементи кібератаки), каналом їх обслуговування – власне група реагування. Математичний апарат такого представлення розглядається в межах марковського процесу. Алгоритмічний опис поданий в операторній формі, де виділено окремі процеси функціонування ГРІБ.

Здійснено імітаційне моделювання для опису часової залежності кількості обслужених (коли протидія кібератакам була здійснена) та втрачених заявок (коли протидія не могла бути здійснена) в залежності від характеристик як кібератак, так і відновлення роботи групи реагування. Показано, що характеристики нелінійно залежать від характеристик моделі: інтенсивності кібератак та її наростання та характеристик відновлення ефективної діяльності ГРІБ.

Розроблена модель надає можливість здійснювати в режимі реального часу оптимальне управління діяльністю ГРІБ в залежності від характеристик кібератак та відновлення діяльності групи реагування, так і від орієнтування керівників на потрібну кількість реагувань чи відмов у реагуванні на інциденти інформаційної безпеки.

Література

1. Crockett M. J. Moral outrage in the digital age / M. J. Crockett // Nature human behaviour. – 2017. – 1(11). – P. 769–771.

2. Wolfsfeld G. The Social Media and the Arab Spring: Politics Always comes First / G. Wolfsfeld, E. Segev, T. Sheafer // The International Journal of Press/Politics. – 2013. – V.18. – P. 115–137.

3. Carley K. M. Social cybersecurity: an emerging science / K. M. Carley // Computational and Mathematical Organization Theory. – 2020. – 26(4). – P. 365–381.

4. Shao, C. The spread of low-credibility content by social bots / C. Shao, G. L. Ciampaglia, O. Varol et al. // Nature Communications. – 2018. – 9. – P. 4787. doi: 10.1038/s41467-018-06930-7.

5. Del Vicario M. The spreading of misinformation online / M. Del Vicario, A. Bessi, F. Zollo, F. Petroni, A. Scala, G. Caldarelli et al. // Proceedings of the National Academy of Sciences. – 2016. – 113(3). – P. 554–559.

6. Allcott H. Social Media and Fake News in the 2016 Election / H. Allcott, M. Gentzkow // Journal of Economic Perspectives. – 2017. – 31 (2). – P. 211–236.

7. Юрков О. С. Психологія праці та інженерна психологія / О. С. Юрков. – Мукачево: МДУ, 2018. – 187 с.

8. Вудсон У. Справочник по инженерной психологии для инженеров и художников-конструкторов / У. Вудсон, Д. Коновер. – М.: Изд-во «МИР», 1968. – 520 с.

9. Котик М. А,. Природа ошибок человека-оператора / М. А. Котик, А. М. Емельянов. – М.: Транспорт, 1993. – 252 с.

10. Вентцель Е. С. Теория случайных процессов и её инженерные приложения / Е. С. Вентцель, Л. А. Овчаров. – М.: Наука. ред. физ.-мат. Лит, 1991. – 384с.

11. Мателыцкий М. Теория вероятности и математическая статистика / М. Мателыцкий, Г. Хацкевич. – М.: ЛитРес, 2021. – 350 с.

12. Бусленко Н. П. Метод статистического моделирования / Н. П. Бусленко. – М.: Статистика, 1970. – 113 с.

13. Каштанов В. А, Медведев А. И. Теория надежности сложных систем / В. А. Каштанов, А. И. Медведев. – М.: ФИЗМАЛИТ, 2010. – 608 с.

14. Кельтон В., Лоу А. Имитационное моделирование. Классика CS / В. Кельтон, А. Лоу. – Киев : Издательская группа BHV, 2004. – 847 с.

15. Копей В. Б. Мова програмування Python для інженерів і науковців / В. Б. Копей. – Івано-Франківськ : ІФНТУНГ, 2019. – 272 с.

References

1. Crockett M. J. Moral outrage in the digital age. Nature human behaviour, 2017, vol. 1(11), pp. 769–771.

2. Wolfsfeld G, Segev E, Sheafer T. The Social Media and the Arab Spring: Politics Always comes First. The International Journal of Press/Politics, 2013, vol. 18, pp. 115–137.

3. Carley K. M. Social cybersecurity: an emerging science. Computational and Mathematical Organization Theory, 2020, vol. 6(4), pp. 365–381.

4. Shao, C., Ciampaglia, G. L., Varol, O., et al. The spread of low-credibility content by social bots. Nature Communications, 2018, vol. 9, pp. 4787. doi: 10.1038/s41467-018-06930-7.

5. Del Vicario M, Bessi A, Zollo F, Petroni F, Scala A, Caldarelli G, et al. The spreading of misinformation online. Proceedings of the National Academy of Sciences, 2016, vol. 113(3), pp. 554–559.

6. Allcott H., Gentzkow M. Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives, 2017, vol. 31 (2), pp. 211-236.

7. Yurkov O. S. Psykholohiya pratsi ta inzhenerna psykholohiya [Labor psychology and engineering psychology]. Mukachevo: MDU, 2018. 187 p.

8. Vudson U., Konover D. Spravochnik po inzhenernoy psikhologii dlya inzhenerov i khudozhnikov-konstruktorov [A Guide to Engineering Psychology for Engineers and Design Artists]. M.: Izd-vo «MIR», 1968. 520 p.

9. Kotik M.A., Yemel'yanov A.M. Priroda oshibok cheloveka-operatora [The nature of human operator error]. M.: Transport, 1993. 252 p.

10. Venttsel' Ye. S., Ovcharov L. A. Teoriya sluchaynykh protsessov i yeyo inzhenernyye prilozheniya [The theory of stochastic processes and its engineering applications]. M.: Nauka. red. fiz.-mat. Lit, 1991. 384 p.

11. Matalytskiy M., Khatskevich G. Teoriya veroyatnosti i matematicheskaya statistika [Probability theory and mathematical statistics]. M. : LitRes, 2021. 350 p.

12. Buslenko N. P. Metod statisticheskogo modelirovaniya [Statistical modeling method]. M.: Statistika, 1970. 113 p.

13. Kashtanov V. A, Medvedev A. I. Teoriya nadezhnosti slozhnykh sistem. [Reliability theory of complex systems]. M. FIZMALIT, 2010. 608 p.

14. Kel'ton V., Lou A. Imitatsionnoye modelirovaniye . Klassika CS [Simulation modeling. Classic CS]. Kiyev : Izdatel'skaya gruppa BHV, 2004. 847 p.

15. Kopey V. B. Mova prohramuvannya Python dlya inzheneriv i naukovtsiv [Python programming language for engineers and scientists]. Ivano-Frankivs′k : IFNTUNH, 2019. 272 p.