https://doi.org/10.31649/1997-9266-2021-159-6-123-130

УДК 35.078.4:519.857.3

І. О. Дьогтєва[1]
А. А. Шиян[1]

МОДЕЛЮВАННЯ РОБОТИ ГРУПИ РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЗРОСТАННЯ ІНТЕНСИВНОСТІ КІБЕРАТАК

[1]Вінницький національний технічний університет

Моделювання функціонування групи реагування на інциденти інформаційної безпеки (ГРІІБ) та прийняття в них рішень саме в процесі протидії кібератакам вимагає одночасного використання параметрів та характеристик, які, з одного боку, характеризують безпосередньо кібератаки та їх розгортання у часі, а, з іншого — вимагають врахування параметрів та показників, які характеризують діяльність спеціалістів в умовах стресової ситуації. Діяльність ГРІІБ полягає у протидії кібератакам, метою яких є дестабілізація соціального стану суспільства шляхом розповсюдження шкідливої інформації. В роботі побудована модель для опису особливостей функціонування ГРІІБ з урахуванням впливу параметра підвищення інтенсивності потоку інцидентів інформаційної безпеки на якість аналізу функціонування цієї системи в реальному часі, використовуючи функції реагування на порушення інформаційної безпеки. Особливістю побудованої моделі є те, що вперше враховано режим перевантаження, тобто враховано вплив введеного параметра підвищення інтенсивності ідентифікації подій інформаційної безпеки. Виявлено умови, за яких здійснюється перехід ГРІІБ до режиму, який не відповідає достатньому критерію ергодичності, коли група не здатна буде ефективно справлятися з розгортанням кібератак у часі. Проведено імітаційне моделювання діяльності ГРІІБ та показано наявність переходу до режиму, породженого відсутністю ергодичної властивості функціонування системи, за зміни параметра підвищення інтенсивності ідентифікації подій інформаційної безпеки. Отримані результати дозволяють прогнозувати появу режиму перевантаження, породженого відсутністю ергодичної властивості функціонування системи, в умовах якого діяльність такої ГРІІБ перестає бути ефективною. Це дозволяє задавати певні порогові величини для часу ефективної діяльності цієї ГРІІБ під час кібератаки. В результаті наявну сукупність ГРІІБ можна характеризувати певними кількісними показниками, які характеризують час ефективної діяльності ГРІІБ в залежності від ідентифікованих характеристик кібератаки. На основі розробленої моделі можуть бути розроблені нові методи протидії кібератакам, які будуть базуватись на ідентифікації потрібних характеристик часового розгортання інциденту кібербезпеки та на їх основі перенаправлення управління від однієї ГРІІБ до іншої в процесі розвитку інциденту. Для цього потрібно буде створити базу даних з потрібними характеристиками для тих ГРІІБ, які можуть бути залучені до процесу протидії кібератакам.

Ключові слова: кібератака, інцидент інформаційної безпеки, група реагування, ефективність протидії.

Вступ

Захист від атак у кіберпросторі з кожним роком набуває все більшої актуальності. Кількість та номенклатура таких атак стрімко зростає, а самі атаки стають щораз різноманітнішими. Розширюють географію комплексні кібератаки, коли зловмисники застосовують цілий набір методів, технологій, інструментів та програмних засобів під час однієї атаки.

Все це призводить до того, що суттєво збільшується навантаження на групи реагування на інциденти інформаційної безпеки (ГРІІБ). Такі групи часто створюють в рамках системи менеджменту інформаційної безпеки (СМІБ), коли виникає необхідність реагувати на інциденти інформаційної безпеки, які мають певні подібні характеристики. Моделювання функціонування ГРІІБ та прийняття в них рішень під час кібератак вимагає одночасного використання параметрів та характеристик кібератак, їх розгортання у часі, а, також урахування параметрів та показників, які характеризують діяльність спеціалістів в даних умовах.

Діяльність ГРІБ з протидії кібератакам полягає в реагуванні на значення параметрів та характеристик, які є характерними для певної атаки. Розглядаються атаки на соціальні системи, коли інформація шкідливого змісту розповсюджується переважно через соціальні мережі. Тому потрібно спочатку ідентифікувати загрозу, розпізнати процес її розгортання у часі, проаналізувати її, розробити систему протидії, підготувати необхідні для розповсюдження матеріали для протидії розгортанню атаки, підготувати ці матеріали та розпочати їх розповсюдження в соціальних мережах. Така діяльність ГРІБ вимагає залучення досить широкого кола експертів та спеціалістів, і часові характеристики її діяльності виділяють такі ГРІБ у окрему категорію.

В загальному випадку, цю діяльність можна представити у вигляді циклічної послідовності таких процесів [1]—[3]: 1) отримання інформації (можна розглядати цей процес як отримання заявки/вимоги на реагування); 2) розробка способу протидії атаці та формування відповідних команд на його виконання (реагування системи на отриману заявку/вимогу).

Враховуючи випадковість у виникненні подій інформаційної безпеки, особливості функціонування ГРІБ можуть моделюватися як марковські процеси на прикладі системи масового обслуговування (СМО) з експоненціально розподіленим часом обробки інцидентів групою і пуассонівським вхідним потоком [4]. Ефективне управління СМО (зміна інтенсивності вхідного потоку, характеристик якості, механізму обслуговування) і безпосередньо їх функціонування вимагає знання як інтенсивностей потоків заявок, які надходять на вхід цих систем, так і їх коливання в часі [4]—[6].

Специфічна особливість системи масового обслуговування ГРІБ полягає в наявності режиму перевантаження, що вперше враховано параметром підвищення інтенсивності подій інформаційної безпеки. Для цього досліджено ланцюг Маркова на відповідність достатньому критерію ергодичності [5] побудованого процесу для діяльності ГРІБ, тобто як параметр підвищення інтенсивності надходження заявок в модельній системі впливає на ергодичну властивість [4].

Ергодична теорія розвивається в межах загальної теорії динамічних систем і вивчає поведінку перетворень з інваріантною мірою. Автори [7], [8] включають в математичну основу ергодичної теорії дослідження умов, за яких системи з невеликою кількістю степенів свободи, які мають статистичні властивості, є ергодичними. В такому випадку ергодичні теореми дають можливість розглядати часові середні на обмеженому чи нескінченному проміжку часу, коли має місце регулярність поведінки динамічних систем, пов’язану з усередненням [7]. У випадку СМО вважається, що граничний розподіл ймовірностей станів ланцюга Маркова не повинен залежати від початкового розподілу і визначається перехідною матрицею, тобто має ергодичну властивість за якої ймовірності станів зі збільшенням переходів практично перестають змінюватись і система переходить у стаціонарний режим функціонування [5].

Метою роботи є моделювання особливостей функціонування ГРІБ в умовах навантаження, зокрема з урахуванням впливу параметра підвищення інтенсивності потоку інцидентів інформаційної безпеки на якість аналізу функціонування цієї системи в реальному часі, використовуючи функції реагування на порушення інформаційної безпеки. Для дослідження умов переходу ГРІБ під час діяльності в режим перевантаження використано достатній критерій ергодичності відповідного марковського процесу. Особливістю побудованої моделі є те, що вперше враховано режим перевантаження, тобто враховано вплив уведеного параметра підвищення інтенсивності ідентифікації подій інформаційної безпеки.

Основна частина

Наведемо алгоритмічний опис поведінки ГРІБ під час кібератаки. Нехай до системи надходить потік заявок на реагування (параметрів, які характеризують часове розгортання однієї кібератаки, або ж кожну окрему кібератаку тощо), причому момент надходження першої заявки є випадкова величина, яка має показниковий розподіл з параметром $\alpha\lambda$, де $\alpha > 0$ (ця складова пов’язана з розвитком кібератак і є кількісною характеристикою збільшення в порівнянні з подібними атаками в минулому періоді, наприклад з причин підвищення рівня складності атаки, використання нових технологій атак тощо). Заявка, яка надійшла на обслуговування, обслуговується випадковий час (аналізується, формується рішення та віддаються команди на його виконання), який має показниковий розподіл з параметром μ. Час надходження наступної заявки є випадкова величина, яка має показниковий розподіл з параметром λ. Якщо до надходження нової заявки система звільняється, то змінюється інтенсивність надходження заявок. Якщо ж нова заявка надійшла раніше, ніж попередня встигла пройти процедуру обслуговування, то вона втрачається.

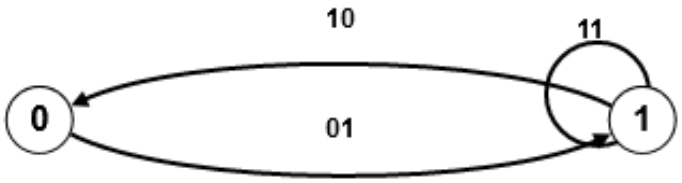


Рис. 1. Граф переходів ГРІБ між станами

Графічний опис структури системи показано на рис. 1.

Система складається з джерела заявок (блок 0) та підсистеми обслуговування (блок 1). Досліджуваний процес і блоки (0, 1) утворюють M/M/1 з діаграмою переходів — 01, 10, 11 [5]. Ця система ускладнюється параметром навантаження через збільшення інтенсивності надходження заявок з блока 0 за умови незайнятості системи.

Наведемо аналітичний опис поведінки наведеної моделі ГРІБ.

Функціонування системи описується марковським процесом $\xi(t)$, множиною станів якого є множина $\{e_0, e_1\}$.

У стані e_0 система перебуває час τ (τ — показниково розподілена випадкова величина з параметром $\alpha\lambda$) і з ймовірністю 1 переходить у стан e_1, тобто в момент τ надійшла заявка, яку передано на обслуговування.

У стані e_1 система перебуває час $\min(\tau',\eta)$, де τ', η — незалежні випадкові величини, зокрема, τ'— час надходження нової заявки (має показниковий розподіл з параметром λ), η — час обслуговування (має показниковий розподіл з параметром μ). Зі стану e_1 система може перейти назад у стан e_0 з ймовірністю

$$p_{10} = P\left(\eta < \tau'\right) = \frac{\mu}{\lambda + \mu} \tag{1}$$

або ж залишитись у стані e_1 з імовірністю

$$p_{11} = P\left(\tau' < \eta\right) = \frac{\lambda}{\lambda + \mu}. \tag{2}$$

Марковський процес $\xi(t)$ у станах e_0, e_1 перебуває відповідно час $\zeta_0 = \tau$, $\zeta_1 = \min(\tau',\eta)$, причому випадкові величини ζ_0, ζ_1 мають показникові розподіли відповідно з параметрами $\alpha\lambda$, $\lambda + \mu$. За визначеності (1), (2), переходи зі стану у стан $\xi(t)$ здійснюється згідно з вкладеним ланцюгом Маркова, який задається матрицею перехідних ймовірностей

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

В рамках досліджуваної системи, де $Q_{ij}(t)$ — ймовірність того, що $\xi(t)$ в i-му стані проведе час менший t і перейде у j-й стан, визначено:

$$\begin{gathered} Q_{00}(t) \equiv 0; \quad Q_{01}(t) = 1 - e^{-\alpha\lambda t}; \\ Q_{10}(t) = \frac{\mu}{\lambda+\mu}\left(1 - e^{-(\lambda+\mu)t}\right); \; Q_{11}(t) = \frac{\lambda}{\lambda+\mu}\left(1 - e^{-(\lambda+\mu)t}\right). \end{gathered} \tag{4}$$

Для

$$P_{ij}(t) = P\left(\xi(t) = j \middle| \xi(0) = i\right) \tag{5}$$

ймовірності того, що процес $\xi(t)$ в момент часу t перебуває у j-му стані за умови, що у початковий момент він перебуває в i-му стані, отримано

$$\begin{gathered} P_{00}(t) = \frac{\mu}{\alpha\lambda+\mu} + \frac{\alpha\lambda}{\alpha\lambda+\mu} e^{-(\alpha\lambda+\mu)t}; \quad P_{01}(t) = \frac{\alpha\lambda}{\alpha\lambda+\mu} - \frac{\alpha\lambda}{\alpha\lambda+\mu} e^{-(\alpha\lambda+\mu)t}; \\ P_{10}(t) = \frac{\mu}{\alpha\lambda+\mu} - \frac{\mu}{\alpha\lambda+\mu} e^{-(\alpha\lambda+\mu)t}; \quad P_{11}(t) = \frac{\alpha\lambda}{\alpha\lambda+\mu} + \frac{\mu}{\alpha\lambda+\mu} e^{-(\alpha\lambda+\mu)t}. \end{gathered} \tag{6}$$

Для функцій (6) виконується $P_{00}(0) = P_{11}(0) = 1$; $P_{01}(0) = P_{10}(0) = 0$; $P_{00}(0) + P_{01}(0) = 1$, $P_{10}(0) + P_{11}(0) = 1$ для всіх t, що узгоджується з їхнім ймовірнісним змістом.

За наявності матриці перехідних ймовірностей ланцюга Маркова зі скінченною множиною станів можна вести мову про ергодичну властивість. Якщо ланцюг Маркова нерозкладний, аперіодичний, з поверненням і додатними елементами, то для нього існує стаціонарний (фінальний) розподіл ймовірностей. Якщо для однорідного ланцюга Маркова існують фінальні ймовірності, то кажуть, що для цього ланцюга існує стаціонарний режим функціонування [6].

Такий режим встановлюється у разі зростання (збільшенні кількості кроків), тобто $t \to +\infty$, в досліджуваній СМО з навантаженням (M/M/1/0 з підвищенням інтенсивності надходження вимоги за умови незайнятості системи) відповідно до ергодичної теореми для ланцюгів Маркова зі зчисленним (скінченним) числом станів [6]

$$\lim_{t\to+\infty} P_{00}(t) = \lim_{t\to+\infty} P_{10}(t) = \frac{\mu}{\alpha\lambda+\mu};$$
$$\lim_{t\to+\infty} P_{01}(t) = \lim_{t\to+\infty} P_{11}(t) = \frac{\alpha\lambda}{\alpha\lambda+\mu}. \quad (7)$$

В нашому випадку ГРІІБ під час протидії кібератакам продовжує переходити зі стану в стан, однак ймовірності цих станів при цьому вже не залежать від початкового розподілу ймовірностей та безпосереднього номера кроку і визначається лише перехідною матрицею (3). Кожний зі станів реалізується з певною постійною ймовірністю (7), яка носить назву ергодичної (граничної або фінальної). Набір цих ймовірностей як координат формує граничний (або фінальний) вектор [5], який моделює, згідно з теорією систем, визначення класу і стану об'єкта.

Можливість отримати граничну ймовірність дозволяє з'ясувати середній відносний час перебування ГРІІБ в такому *i*-му стані, зокрема, в умовах функціонування ГРІІБ під час протидії кібератакам. Результати

$$\pi_0 = \frac{\mu}{\alpha\lambda+\mu}; \quad \pi_1 = \frac{\alpha\lambda}{\alpha\lambda+\mu} \quad (8)$$

дозволяють описати протягом досить значного проміжку часу $(0;T)$ процес $\xi(t)$, який буде перебувати у станах e_0, e_1, такий час, який оцінюється числами $\pi_0 T$, $\pi_1 T$. Для ГРІІБ під час протидії кібератакам, функціонування якої описується процесом $\xi(t)$, протягом проміжку часу $(0;T)$ у середньому буде незайнятою приблизно час $\pi_0 T$, і зайнятою обслуговуванням приблизно час $\pi_1 T$.

Для розгляду ергодичної властивості математичної моделі ГРІІБ використано програмну реалізацію імітаційної моделі для M/M/1 з втратами (одноканальна СМО з відмовами) та досліджуваної моделі ГРІІБ, тобто для M/M/1/0 з підвищенням інтенсивності надходження заявки за умови незайнятості системи (модель СМО з навантаженням). Для цієї реалізації використано мову програмування Python [9].

До переліку вхідних даних (рис. 2) моделі ГРІІБ включені: інтенсивність потоку заявок (інтенсивність надходження заявок), яка доповнюється параметром навантаження (параметр підвищення інтенсивності надходження заявок), продуктивність каналу (сервера) обслуговування заявок (інтенсивність обслуговування заявок) та кількість циклів для проведення сценаріїв експериментів.

```
Model M/M/1 with increasing intensity of demand receipt on condition of system idleness
Output data:
Intensity of the receipt of requests                              : 3
The parameter to increase the intensity of the receipt of requests      : 4
Intensity of service of requests                                  : 5
Number of cycles for each experiment                              : 100
-------------------------------------------------------------------------------------------------
system_characteristics                  M/M/1                 M/M/1 with increasing intensity
-------------------------------------------------------------------------------------------------
Average time of receipt of the request:          0.333                    0.083
Average service time requirements:               0.2                      0.2
Average time spent by a request in the system:   0.125                    0.059
Relative bandwidth:                              0.625                    0.294
Absolute bandwidth:                              1.875                    3.529
The probability that the channel is busy:        0.375                    0.706
The intensity of the flow of lost requirements:  1.125                    8.471
-------------------------------------------------------------------------------------------------
```

Рис. 2. Приклад вхідних даних та системні характеристики M/M/1 та M/M/1/0 (модель ГРІІБ) з підвищенням інтенсивності надходження заявки за умови незайнятості системи

Запропонована математична модель пов'язує задані умови роботи ГРІІБ з показниками ефективності, в якості яких аналітично розраховані [10] величини таких характеристик (рис. 2): середній час надходження та обслуговування вимоги, середній час перебування заявки в системі, частки обслужених та не обслужених заявок в загальній кількості, інтенсивності потоку втрачених та обслужених вимог у граничному випадку.

Параметр підвищенням інтенсивності надходження заявки природно зумовив зменшення очікуваного часу між двома послідовними заявками (збільшив інтенсивність) та скорочення серед-

нього часу перебування заявки в системі.

Частки обслужених та необслужених заявок в загальній кількості відповідають стаціонарним характеристикам систем (8), в порівнянні спостерігається різниця за безпосередньо даною вхідною інформацією в майже 33,1 % (зменшення пропускної спроможності в умовах збільшення навантаження на систему в показник параметра підвищення інтенсивності надходження заявок). Експериментальні дослідження за цим експериментом практично підтвердили теоретичний результат (рис. 3) для значень стаціонарних характеристик (8).

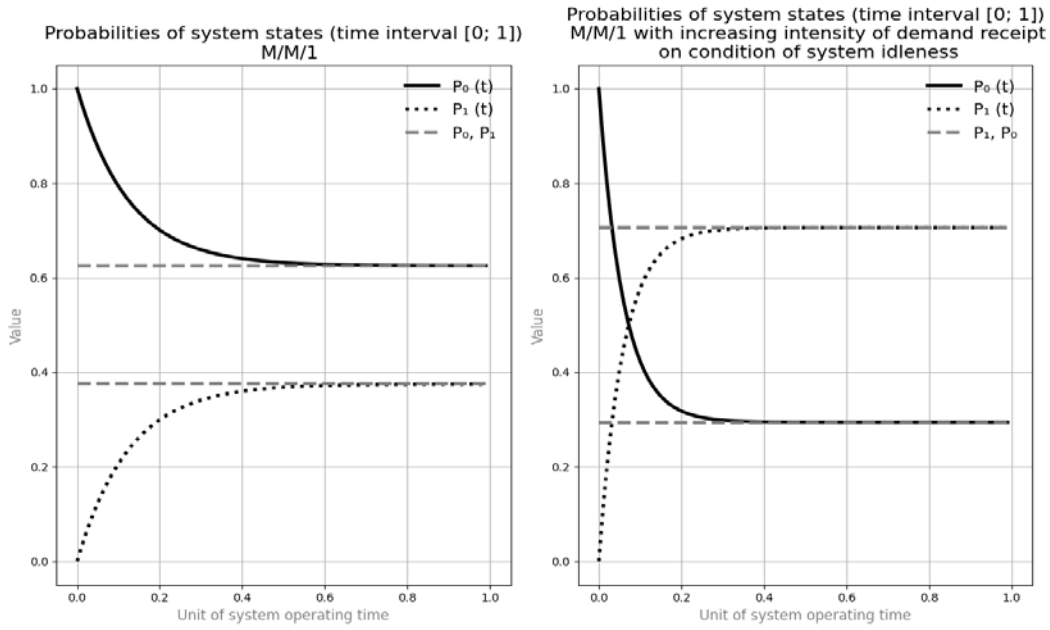
static_characteristics	theoretical_intensive_requests	practical_intensive_requests
π_0	0.2941	0.2935
π_1	0.7059	0.7065
total_system_uptime	-	22.09

Рис. 3. Значення стаціонарних характеристик для M/M/1/0 (модель ГРІБ) з підвищенням інтенсивності надходження заявки за умови незайнятості системи

Зміни у значеннях інтенсивності потоку втрачених, обслужених вимог (абсолютна пропускна спроможність) в граничному випадку залежать від змін значень стаціонарних характеристик, а також від параметра підвищення інтенсивності надходження заявок.

Загалом в подібних ситуаціях для аналізу системи достатньо вихідних даних, але в нашому випадку досить важливо мати інформацію про поведінку системи на початковому часовому інтервалі. Це дозволить оперативно приймати рішення щодо підвищення ефективності роботи ГРІБ з інформаційного захисту системи.

На рис. 4 подана візуалізація даних імітаційного експерименту, зокрема, графіки ймовірностей станів системи в межах часового інтервалу [0; 1] — одиниця часу роботи системи для, відповідно, M/M/1 та M/M/1/0 (модель ГРІБ) з підвищенням інтенсивності надходження вимоги за умови незайнятості системи.



а *б*

Рис. 4. Графіки ймовірностей станів системи на часовому інтервалі [0; 1] для систем: *а* — M/M/1; *б* — M/M/1/0 (модель ГРІБ) з підвищенням інтенсивності надходження вимоги за умови незайнятості системи

Візуалізація демонструє, що відповідні графіки досить швидко виходять на асимптотичні (постійні) значення, які відповідають граничним значенням (відносній пропускній спроможності та ймовірності того, що канал зайнятий), показаних на рис. 2. На цих графіках показані два з трьох можливих варіантів рішень за різних відношень між інтенсивністю вхідного потоку та інтенсивністю обслуговування:

– для системи M/M/1 (рис. 4*а*) виконується умова $\lambda < \mu$ (система частіше вільна, аніж зайнята

обслуговуванням заявок), тобто робота системи переходить в стаціонарний режим;

– система M/M/1/0 (модель ГРІБ) з підвищенням інтенсивності надходження вимоги за умови незайнятості системи (рис. 4*б*) перебуває в нестабільному режимі функціонування, де інтенсивність надходження заявок перевищує інтенсивність обслуговування $\alpha\lambda > \mu$, тобто параметр підвищення інтенсивності надходження заявок призвів до режиму перевантаження).

Таким чином, параметр підвищення інтенсивності надходження заявок в модельній системі впливає на ергодичну властивість системи [4], [8]. Робота системи в нормальному стані представляла ергодичний процес, в яким отримані імовірності станів системи не залежать від того, у якому стані система була у початковий момент. Навантаження системи заявками викликало невиконання достатнього критерію ергодичності марковського процесу [5], що може призвести до того, що після досить тривалого часу функціонування системи може не наступити стаціонарний режим, де імовірність того, що система буде в *k*-му стані, не залежить від того, у якому стані вона знаходилася в початковий момент часу.

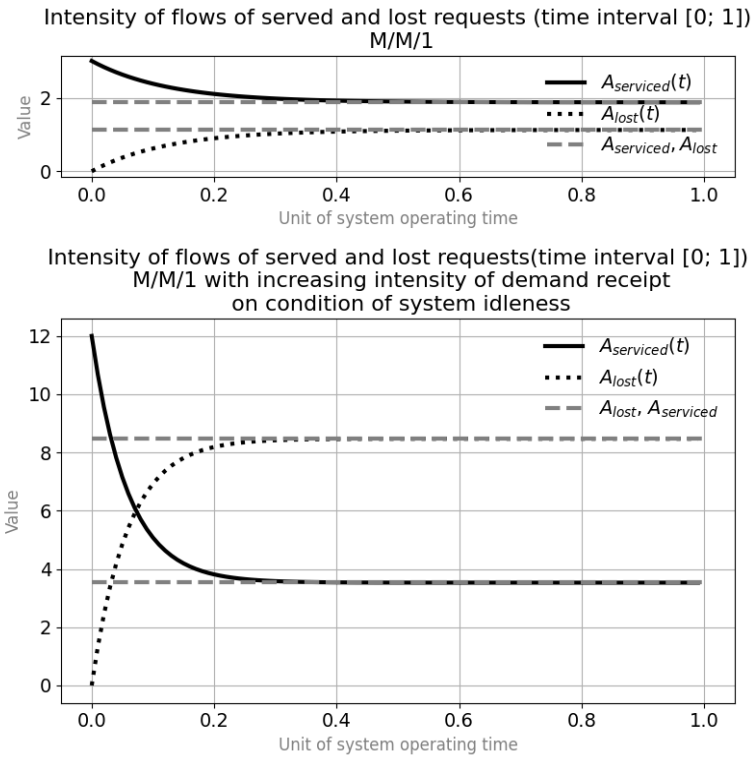


Рис. 5. Графіки інтенсивності потоків обслужених та втрачених заявок на інтервалі [0; 1] для: а) M/M/1; б) M/M/1/0 (модель ГРІБ) з підвищенням інтенсивності надходження вимоги за умови незайнятості системи

Загалом же для системи (ГРІБ) в середньому або має надходити менше вимог ніж вона їх може обслужити, або середня кількість вимог за одиницю часу обслуговування не повинна перевищувати кількості каналів (наприклад, серверів).

Графіки інтенсивності потоків обслужених та втрачених заявок для відповідно M/M/1 та M/M/1/0 (модель ГРІБ) з підвищенням інтенсивності надходження вимоги за умови незайнятості системи (рис. 5) аналогічно з попередніми графіками, показані в діапазоні одиниці часу роботи системи. Цей часовий інтервал дозволяє спостерігати фактичний перехід у стаціонарний режим через наближення до асимптот, тобто аналітично розрахованих значень інтенсивності потоків втрачених та обслужених вимог (абсолютна пропускна спроможність) в граничному випадку (рис. 5).

Висновки

Отримані результати дозволяють прогнозувати появу режиму перевантаження, породженого відсутністю ергодичної властивості функціонування системи, в умовах якого діяльність цієї ГРІБ перестає бути ефективною. Це дозволяє задавати певні порогові величини для часу ефективної діяльності даної ГРІБ під час кібератаки. В результаті наявну сукупність ГРІБ можна характеризувати певними кількісними показниками, які характеризують час ефективної діяльності такої ГРІБ в залежності від ідентифікованих характеристик кібератаки.

Це дозволяє оптимізувати діяльність щодо протидії інцидентам інформаційної безпеки шляхом передачі в процесі розгортання кібератаки управління протидією тим ГРІБ, які будуть ефективнішими на цьому етапі її розгортання. Можливо, в деяких випадках це буде виражено просто в заміні чи залученні одного чи декількох додаткових спеціалістів вищого рівня. А в деяких випадках все управління інцидентом буде передаватися новій, ефективнішій ГРІБ.

На основі запропонованої моделі можуть бути розроблені нові методи протидії кібератакам, які будуть базуватись на ідентифікації потрібних характеристик часового розгортання інциденту кібе-

рбезпеки та на їх основі перенаправлення управління від однієї ГРІБ до іншої в процесі розвитку інциденту. Для цього потрібно буде створити базу даних з потрібними характеристиками для тих ГРІБ, які можуть бути залучені до процесу протидії кібератакам.

Подальші дослідження також можуть здійснюватися в напрямку продовження аналізу поведінки функціонування ГРІБ в умовах навантаження з урахуванням впливу параметра підвищення інтенсивності потоку інцидентів інформаційної безпеки. З метою отримання потрібних статистичних даних, варто здійснити серію імітаційних моделювань з суттєвим збільшенням проведених експериментів, які будуть наближені до практичних ситуацій. Для цього можна залучати дані хабів для досліджень та відпрацювання заходів протидії гібридним впливам в кіберпросторі. Також потрібне подальше дослідження функцій відновлення потоків обслужених та втрачених заявок.

Перспективним також є моделювання роботи ГРІБ в умовах навантаження з регулюванням показника ефективності роботи групи. Інформація щодо критичних значень параметра підвищення інтенсивності потоку інцидентів інформаційної безпеки для ГРІБ із заданими вхідними параметрами дозволяє як виявляти та блокувати режим перевантаження шляхом, так і вносити зміни в роботу ГРІБ через прийняття менеджерських рішень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] В. І. Андреєв, В. О. Хорошко, В. С. Чередниченко, і М. Є. Шелест, *Основи інформаційної безпеки*. Київ, Україна: вид. ДУІКТ, 2009.

[2] В. І. Андреєв, В. Д. Козюра, Л. М. Скачек, і В. О. Хорошко, *Стратегія управління інформаційною безпекою*. Київ, Україна: ДУІКТ, 2007.

[3] М. В. Белов, и Д. А. Новиков, *Модели деятельности (основы математической теории деятельности)*. Москва, РФ: Ленанд, 2021.

[4] Е. С. Вентцель, и Л. А. Овчаров, *Теория случайных процессов и её инженерные приложения*. Москва: Наука. ред. физ.-мат. лит, 1991.

[5] О. Є. Голоскоков, А. О. Голоскокова, і Є. О. Мошко, *Основи теорії експоненціальних систем масового обслуговування*. Харків, Україна: НТУ «ХПІ», 2017.

[6] М. Маталыцкий, и Г. Хацкевич, «*Теория вероятности и математическая статистика*,» ЛитРес, 2021. [Электронный ресурс] Режим доступу: https://www.litres.ru .

[7] Т. В. Кілочицька, «Еволюція ергодичної теорії,» *Наука та наукознавство*, № 7 (106), с. 102-115, 2019.

[8] Я. Г. Синай, И. П. Корнфельд, и С. В. Фомин, *Эргодическая теория*. Москва: Наука, 1980.

[9] В. Б. Копей, *Мова програмування Python для інженерів і науковців*. Івано-Франківськ, Україна: ІФНТУНГ, 2019.

[10] В. Кельтон, и А. Лоу, *Имитационное моделирование. Классика CS*. 3-е изд . СПб, РФ: Питер; Киев, Украина: Издательская группа BHV, 2004.

Рекомендована кафедрою менеджменту та безпеки інформаційних систем ВНТУ

Стаття надійшла до редакції 09.12.21

Дьогтєва Ірина Оксентіївна — асистент кафедри менеджменту та безпеки інформаційних систем;

Шиян Анатолій Антонович — канд. фіз.-мат. наук, доцент, доцент кафедри менеджменту та безпеки інформаційних систем, e-mail: anatoliy.a.shiyan@gmail.com

I. O. Dohtieva[1]
A. A. Shyian[1]

Simulation of the Work of the Information Security Incident Response Group in the Conditions of Increasing Cyberattack Intensity

[1]Vinnytsia National Technical University

Modeling of the Information Security Incident Response Team (ISIRT) functioning and decision-making in the process cyberattacks requires the simultaneous use of parameters and characteristics at, on the one hand, directly characterize cyberattacks and their deployment over time, and, on the other hand, require taking into account the parameters and indicators that characterize the activities of specialists in a stressful situation. ISIRT's activities are to counter cyberattacks aimed at destabilizing the social state of society by disseminating harmful information. The paper builds a model to describe the features of the ISIRT, taking into account the impact of the parameter of increasing the intensity of information security incidents on the quality of analysis of the system in real time, using the functions of responding to information security violations. The peculiarity of the constructed model is that for the first time the overload mode is taken into account, i.e. the influence of the introduced parameter of increasing the intensity of information security event identification is taken into account.

The conditions under which the ISIRT is transitioning to a regime that does not meet the sufficient criterion of ergodicity, when the group will not be able to effectively cope with the deployment of cyber attacks in time. Simulation modeling of ISIRT activity is carried out and the presence of transition to the mode, which is caused by the lack of ergodic property of the system functioning, when changing the parameter of increasing the intensity of information security event identification, is shown. The obtained results allow predicting the appearance of the overload mode caused by the lack of ergodic properties of the system operation, in the conditions of which the activity of this ISIRT ceases to be effective. This allows you to set certain thresholds for the time of effective operation of this ISIRT during a cyber attack. As a result, the existing set of ISIRT can be characterized by certain quantitative indicators that characterize the time of effective operation of this ISIRT, depending on the identified characteristics of the cyber attack. Based on the developed model, new methods of countering cyberattacks can be developed, which will be based on identifying the required characteristics of the temporal deployment of cybersecurity incidents and on their basis redirecting control from one ISIRT to another during the incident. This will require the creation of a database with the necessary characteristics for those ISIRTs that may be involved in the process of countering cyberattacks.

Keywords: cyberattack, information security incident, response team, effectiveness of counteraction.

Dohtieva Iryna O. — Assistant of the Chair of Management and Security of Information Systems;
Shyian Anatolii A. — Cand. Sc. (Phys.-Math.), Associate Professor, Associate Professor of the Chair of Management and Security of Information Systems, e-mail: anatoliy.a.shiyan@gmail.com

И. А. Дёгтева[1]
А. А. Шиян[1]

Моделирование работы группы реагирования на инциденты информационной безопасности в условиях роста интенсивности кибератак

[1]Винницкий национальный технический университет

Моделирование функционирования группы реагирования на инциденты информационной безопасности (ГРИИБ) и принятие в них решений именно в процессе противодействия кибератакам требует одновременного использования параметров и характеристик, которые, с одной стороны, характеризуют непосредственно кибератаки и их развертывание во времени, а с другой — требуют учет параметров и показателей, характеризующих деятельность специалистов в условиях стрессовой ситуации. Деятельность ГРИИБ заключается в противодействии кибератакам, целью которых является дестабилизация социального положения общества путем распространения вредоносной информации.

Построена модель для описания особенностей функционирования ГРИИБ с учетом влияния параметра повышения интенсивности потока инцидентов информационной безопасности на качество анализа функционирования данной системы в реальном времени, используя функции реагирования на нарушение информационной безопасности. Особенностью построенной модели является то, что впервые учтен режим перегрузки, то есть учтено влияние параметра повышения интенсивности идентификации событий информационной безопасности. Выявлены условия, при которых осуществляется переход ГРИИБ к режиму, не отвечающему достаточному критерию эргодичности, когда группа не способна будет эффективно справляться с развертыванием кибератак во времени. Проведено имитационное моделирование деятельности ГРИИБ и показано наличие перехода к режиму, порожденному отсутствием эргодичного свойства функционирования системы, с изменением параметра повышения интенсивности идентификации событий информационной безопасности. Полученные результаты позволяют прогнозировать появление режима перегрузки, порожденного отсутствием эргодического свойства функционирования системы, в условиях которого деятельность ГРИИБ перестает быть эффективной. Это позволяет задавать определенные пороговые величины времени эффективной деятельности данной ГРИИБ во время кибератаки. В результате имеющуюся совокупность ГРИИБ можно характеризовать определенными количественными показателями, характеризующими время эффективной деятельности этой ГРИИБ в зависимости от идентифицированных характеристик кибератаки. На основе разработанной модели могут быть разработаны новые методы противодействия кибератакам, которые будут основываться на идентификации нужных характеристик временного развертывания инцидента кибербезопасности и на их основе перенаправления управления от одной ГРИИБ к другой в процессе развития инцидента. Для этого нужно будет создать базу данных с необходимыми характеристиками для тех ГРИИБ, которые могут быть вовлечены в процесс противодействия кибератакам.

Ключевые слова: кибератака, инцидент информационной безопасности, группа реагирования, эффективность противодействия.

Дёгтева Ирина Аксентьевна — ассистент кафедры менеджмента и безопасности информационных систем;
Шиян Анатолий Антонович — канд. физ.-мат. наук, доцент, доцент кафедры менеджмента и безопасности информационных систем, e-mail: anatoliy.a.shiyan@gmail.com