DOI: 10.35681/1560-9189.2021.23.4.265720

УДК 519.857.3

І. О. Дьогтєва, А. А. Шиян, В. С. Катаєв
Вінницький національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

Моделювання відновлення ефективної діяльності групи реагування на інциденти інформаційної безпеки в умовах наростання інтенсивності кібератак

Останнім часом стрімко зростає кількість випадків використання кіберпростору для кібератак як на окремих людей, соціальні групи, так і на суспільство в цілому. Такі атаки характеризуються тим, що їхня інтенсивність зростає протягом атаки. Внаслідок цього складаються нові умови для діяльності груп реагування на інциденти інформаційної безпеки (ГРІБ). Однак ефективність діяльності ГРІБ, яка здійснюється протягом тривалого часу, зменшується внаслідок цілого ряду причин, зокрема втоми спеціалістів. У статті здійснено моделювання особливостей функціонування ГРІБ в умовах наростання інтенсивності кібератак з урахуванням впливу параметрів і характеристик їхнього відновлення, що є необхідним для ефективного функціонування даної групи. Отримано функцію відновлення пуассонівського потоку та щільність її відновлення, запропоновано формули для функцій відновлення потоку обслужених і втрачених заявок для процесу відновлення ГРІБ під час кібератак. Особливість побудованої для дослідження моделі полягає у врахуванні параметра підвищення інтенсивності ідентифікації подій інформаційної безпеки. Проведено імітаційне моделювання діяльності ГРІБ, яке показало, що показники зміни ефективності їхньої діяльності в процесі протидії кібератакам із наростанням інтенсивності можуть бути прогнозовані з використанням отриманих результатів.

Ключові слова: *кібератака, інцидент інформаційної безпеки, група реагування, наростання інтенсивності, процес відновлення.*

Вступ

З розвитком інформаційних технологій усе більше напрямків діяльності людини переходить до кіберпростору. Спілкування людей сьогодні все більше обмежується соціальними мережами: сьогодні навіть ЗМІ, теле- та радіотрансляції, прокат кінофільмів здійснюються саме через дані канали комунікацій. По суті, на

теперішньому етапі розвитку соціальних мереж, вони стають силою, яка визначає напрямки діяльності як окремої особи, так і соціальних груп і суспільства в цілому.

Якщо раніше атаки на соціальну сферу суспільства здійснювалися переважно через паперові ЗМІ, книги, радіо та телебачення, то сьогодні для цього використовується кіберпростір. Таким чином, сьогодні все більша кількість інцидентів інформаційної безпеки, метою яких є саме вплив на соціальне середовище, використовують кіберпростір. А це, в свою чергу, висуває нові вимоги до функціонування груп реагування на інциденти інформаційної безпеки (ГРІІБ). Зокрема, виникає вимога як в залученні спеціалістів із часто вельми різних сфер знань і вмінь, так і до організації їхньої спільної діяльності під час реагування на кібератаки (а вони у соціальній сфері можуть тривати досить великі проміжки часу).

Огляд літератури

Наведено кілька прикладів успішного впливу на суспільство, яке було здійснено з використанням кіберпростору, зокрема соціальних мереж. У [1, 2] розглянуто вплив соціальних мереж на здійснення революції в Єгипті у 2011 році та інші протестні акції так званої «Арабської весни». Автори [1] «по гарячих слідах» революції в Єгипті відмічають, що «соціальні медіа відіграли важливу роль в успіху антиурядових протестів» (тут і надалі переклад авторів). У статті [2] в результаті аналізу з використанням баз даних із двадцяти арабських країн і Палестинської автономії виявили справедливість двох тверджень. Перше полягає в тому, що при вивченні ролі соціальних медіа потрібно враховувати роль політичного контексту. Друге — що інтенсивність використання каналів комунікації відслідковує інтенсивність протестної активності. А така діяльність вимагає спеціальної організації діяльності груп реагування на інциденти інформаційної безпеки.

Кібератаки на соціальне середовище часто використовують фейки та дезінформацію [3–6]. Таке розповсюдження має свої особливості. В [3] використано велику базу даних Facebook для порівняльного аналізу розповсюдження мережею коректної (наукові новини) та фейкової (новини зі сфери конспірології) інформації. Автори виявили, що «хоча споживачі наукових історій і конспірологічних історій представляють подібні моделі споживання щодо вмісту, каскадна динаміка відрізняється. Вибірковий вплив вмісту є основним драйвером розповсюдження вмісту та породжує утворення однорідних кластерів, тобто «ехокамер». У [4] здійснено аналіз 14 мільйонів повідомлень, які поширювали 400 тисяч статей у Twitter протягом десяти місяців у 2016 та 2017 роках. Результати дослідження дозволили виявити ряд важливих закономірностей щодо використання ботів для розвитку кібекратак: «соціальні боти відігравали непропорційно велику роль у поширенні статей із джерел низької довіри. Боти посилюють такий вміст на ранніх етапах поширення, до того, як стаття стане вірусною. Вони також націлені на користувачів з великою кількістю підписників за допомогою відповідей і згадок. … стримування соціальних ботів може бути ефективною стратегією для пом'якшення поширення дезінформації в Інтернеті».

У [5] звертається увага на те, що «сайти соціальних мереж сприяють політичній поляризації, створюючи «ехокамери», які ізолюють людей від протилежних поглядів на поточні події». За результатами спеціально проведеного натурного експерименту з опитування прихильників республіканської і демократичної пар-

тій США, які активно користуються Twitter, автори виявили: «республіканці, які підписалися на ліберального бота в Twitter, стали значно консервативнішими після експерименту. Демократи продемонстрували невелике зростання ліберальних настроїв після того, як перейшли на консервативного бота в Twitter, хоча ці ефекти не є статистично значущими». Відмітимо, що ці результати перегукуються з результатами статті [2], яка досліджувала процеси в інших країнах.

У статті [6] проведено імітаційне моделювання та отримано кількісні дані щодо можливого впливу ботів на формування суспільної думки: «в дуже поляризованій обстановці, залежно від загальної щільності мережі, участь лише 2–4 % ботів може бути достатньою, щоб змінити клімат думок. … Ці результати демонструють механізм, за допомогою якого боти можуть формувати норми, які потім приймаються користувачами соціальних мереж.»

Нарешті, в [7] аналізується стан досліджень із впливу соціальних мереж на окрему людину, соціальні групи та суспільство в цілому і стверджується, що «З'являється нова наукова та інженерна дисципліна — соціальна кібербезпека.»

Таким чином, робота ГРІБ в умовах необхідності реагування на інформаційні інциденти, що впливають на суспільство, буде продовжуватися досить тривалий час, причому зі зростанням інтенсивності. До неї потрібно залучати широкий спектр спеціалістів, оперувати багатьма різнорідними базами даних. Подібні умови є досить нетиповим режимом діяльності для ГРІБ.

Питання оптимізації роботи ГРІБ останнім часом привертають усе більшу увагу дослідників. Так, у [8] звертається увага на те, що для ефективної роботи ГРІБ необхідно формування спеціалізованих баз даних, які повинні постачатися як результати звітів таких груп за результатами їхньої роботи. В дослідженні зазначено, що: «ці команди більше зосереджуються на ліквідації та відновленні і менше на наданні зворотного зв'язку для підвищення безпеки організації. Це наводить на думку, що дані, зібрані під час розслідування інцидентів безпеки, можуть бути недостатньо якісними для аналізу розвідки загроз». Автори в [9] стверджують, що «література щодо виявлення інцидентів кібербезпеки та реагування на них дуже багата методологіями автоматичного виявлення, зокрема, заснованими на парадигмі виявлення аномалій. Проте діагностиці методів, спрямованих на надання корисної інформації про причини даної виявленої аномалії, приділено дуже мало уваги. Ця інформація надзвичайно важлива для групи безпеки, щоб скоротити час від виявлення до реагування». В [10] підтверджується попередня думка: «Культурні та безпекові настрої щодо зовнішнього спостереження, а також проблеми з публікацією обмежують здатність дослідників зрозуміти контекст реагування на інцидент. Усвідомлення контексту має вирішальне значення при інформуванні, проектуванні та інженерії». Дослідження [11] виявило, що «автоматизоване сортування інцидентів у великих хмарних сервісах стикається з багатьма проблемами: 1) дуже незбалансований розподіл інцидентів від великої кількості команд; 2) широкий спектр форматів вхідних даних або джерел даних; 3) масштабування для забезпечення продуктивності, вимоги до оцінки; 4) завоювання довіри інженерів до використання рекомендацій машинного навчання».

Для підвищення ефективності роботи ГРІБ у [12] пропонується «інтеграція функцій управління інформаційною безпекою та реагування на інциденти». Це буде створювати «можливості для навчання, які призводять до переваг організа-

ційної безпеки, включаючи: підвищення обізнаності про ризики безпеки, компіляцію інформації про загрози, усунення недоліків у захисті безпеки, оцінку логіки захисту та посилення безпеки.»

Отже, виникає необхідність у вивченні особливостей функціонування ГРІБ у нових умовах. Такими умовами, зокрема, є необхідність тривалого підтримування ефективної роботи ГРІБ. Як свідчать результати проведеного огляду літератури, змінюються умови роботи ГРІБ: підвищується напруженість роботи спеціалістів, вимоги до їхніх когнітивних і творчих можливостей [13, 14], вимоги до зберігання високого рівня уваги під час роботи тощо. Адже в умовах комплексних кібератак деякі їхні важливі елементи можуть бути невірно або неякісно ідентифіковані [8–12]. Усе це призводить до того, що спеціалісти ГРІБ можуть досягати стану виснаження, коли їхні психологічні та фізіологічні ресурси, їхні адаптаційні та когнітивні можливості щодо опрацювання нової та стрімко змінюваної інформації вже не дають їм можливості ефективно реагувати на зміну ситуації. Тобто настає час, коли вони повинні відпочити, щоб відновитися [13–15]. У цьому випадку для ефективної роботи ГРІБ або необхідно підвищити навантаження для все ще працездатних спеціалістів, або ж організувати поповнення ГРІБ новими спеціалістами.

Основною вимогою до діяльності ГРІБ є ефективність її роботи під час реагування на кібератаки. Особливо це стає критичним в умовах наростання інтенсивності кібератак, коли можливості ефективного виконання обов'язків спеціалістами зменшуються з часом. Слід підкреслити, що така ситуація відмови навіть для одного й того ж спеціаліста, навіть в умовах аналогічного наростання інтенсивності аналогічної кібератаки, настає через різні проміжки часу [13–15]. Аналогічна ситуація притаманна і для часу відновлення. При цьому враховуються різні впливи як психологічного, так і фізіологічного характеру [13–15].

Таким чином, складні умови функціонування кіберпростору, номенклатурна насиченість і комплексність кібератак вимагають наукового дослідження таких аспектів реалізації діяльності ГРІБ як відновлення працездатності їхніх спеціалістів. При цьому як час відмови, так і час відновлення ефективної роботи ГРІБ, є випадковою величиною. Внаслідок цього, відповідний режим функціонування ГРІБ можна моделювати в рамках системи масового обслуговування (СМО) з експоненціально розподіленими як часом виходу з ладу, так і часом відновлення [16, 17]. Такі моделі дозволяють отримати кількісні показники та характеристики, які є важливими для управління ефективним функціонуванням ГРІБ.

Мета роботи.

Провести моделювання особливостей функціонування ГРІБ в умовах наростання інтенсивності кібератак з урахуванням впливу параметрів і характеристик їхнього відновлення, що є необхідним для ефективного функціонування даної групи.

Базова модель.

Наведемо алгоритмічний опис процесу відновлення ГРІБ в умовах наростання інтенсивності кібератак, розглядаючи їх як СМО з відновленням.

Розглянемо потік заявок на реагування (параметрів, які характеризують часове розгортання комплексної кібератаки, або ж кожну окрему кібератаку), що описується законом Пуассона з параметром інтенсивності $\alpha\lambda$, де $\alpha > 0$ — складова, що пов'язана з розвитком кібератак і виступає як кількісна характеристика збільшення їхньої інтенсивності (наприклад, з причин підвищення рівня складності атаки, використання нових технологій атак тощо).

Заявки реєструються ГРІБ, яка працює в наступному режимі. На початку атак ГРІБ не обробляє інциденти інформаційної безпеки (заявки). Враховуючи випадковість у виникненні інцидентів інформаційної безпеки, після певного випадкового часу τ_1, експоненціально розподіленого з параметром $\alpha\lambda$, де $\alpha > 0$, до системи надходить заявка, яка реєструється. Потім заявка обслуговується протягом випадкового часу η_2 (аналізується, виробляється рішення та віддаються команди на його виконання), який має показниковий розподіл з параметром μ. Тобто ГРІБ блокується на певний проміжок часу, протягом якого наступні заявки не реєструються. В цей час заявка не тільки обробляється, але й виділяється певний проміжок часу для відновлення працездатності спеціалістів ГРІБ (цей час також є випадковим і залежить від складності опрацювання заявки). Часом надходження наступної заявки є випадкова величина τ_2', яка має показниковий розподіл з параметром λ. Якщо до надходження нової заявки система звільняється, то змінюється інтенсивність надходження заявок. Після того як ГРІБ звільняється, чергова заявка, що з'явилася після часу τ_2, реєструється. Якщо ж нова заявка надійшла раніше, ніж попередня встигла пройти процедуру обслуговування, то вона втрачається. Далі цикл повторюється. Таким чином, ГРІБ моделюється системою масового обслуговування, яка позначається як M/M/1/0 [17] (рис. 1).

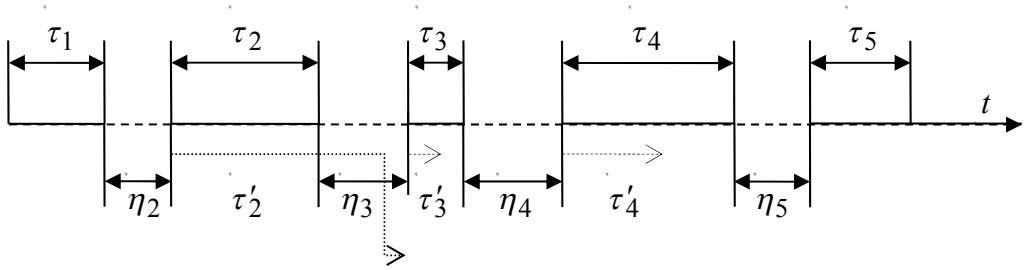

Рис. 1. Ілюстрація роботи M/M/1/0 (модель ГРІБ) з підвищенням інтенсивності надходження заявки за умови незайнятості системи

Враховуючи різні статистичні характеристики послідовностей випадкових величин $\{\tau_1, \tau_2, ...\}$, $\{\eta_2, \eta_3, ...\}$ з урахуванням $\{\tau_2', \tau_3', ...\}$, отримуємо різні процеси відновлення.

Оскільки виникнення інцидентів інформаційної безпеки має пуассонівський характер, то випадкові величини $\{\tau_1, \tau_2, ...\}$ є незалежними та однаково експоненціально розподіленими з параметром $\alpha\lambda$. Аналогічно часові проміжки блокування $\min(\tau', \eta)$ також незалежні і однаково розподілені зі щільністю ймовірності $\lambda + \mu$. У даному випадку обидві послідовності випадкових величин взаємонеза-

лежні. Отже, по суті маємо опис марківського процесу $\xi(t)$, який перебуває у станах e_0, e_1 відповідно час $\zeta_0 = \tau$, $\zeta_1 = \min(\tau', \eta)$, причому випадкові величини ζ_0, ζ_1 мають показникові розподіли відповідно з параметрами $\alpha\lambda$, $\lambda + \mu$ для системи масового обслуговування з навантаженням, зокрема, для M/M/1/0 із підвищенням інтенсивності надходження заявки за умови незайнятості системи.

Для даних процесів відновлення зміна станів (типів інтервалів) описується ланцюгом Маркова [16] $\xi(t)$ з двома станами $\{e_0, e_1\}$ з матрицею ймовірностей переходу:

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

Відповідно до (1), у стані e_0 система перебуває час τ (τ — показниково розподілена випадкова величина з параметром $\alpha\lambda$) і з імовірністю 1 переходить до стану e_1 (тобто в момент τ надійшла заявка 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 до стану e_0 з імовірністю $p_{10} = P(\eta < \tau')$, або ж залишитись у стані e_1 з імовірністю $p_{11} = P(\tau' < \eta)$.

Наведемо математичний опис функцій відновлення для процесу відновлення.

Оскільки ймовірність випадкової величини $v(t)$ — числа заявок, які надходять за час t, для заданого пуассонівського потоку ($k = 0,1,2,...$) має вигляд

$$P(v(t) = k) = \frac{(\alpha\lambda t)^k}{k!} e^{-\alpha\lambda t}, \tag{2}$$

то для процесу відновлення маємо математичне очікування числа відновлень, що відбулися до моменту t, $t \geq 0$:

$$Mv(t) = \sum_{k=0}^{\infty} kP(v(t) = k) = \alpha\lambda t. \tag{3}$$

Функція відновлення визначається як математичне очікування числа відновлень (попадань марківського процесу в певний стан), що відбулися до t [17, 18]. У випадку пуассонівського потоку з параметром $\alpha\lambda$, дана функція відновлення буде мати вигляд:

$$H(t) := Mv(t) = \alpha\lambda t. \tag{4}$$

Для (4) щільність відновлення (інтенсивність надходження заявок):

$$h(t) = H'(t) = \alpha\lambda. \tag{5}$$

Для $v_s(t)$ — числа заявок, які пройшли процедуру обслуговування за час t, та $v_l(t)$ — числа заявок, які були втрачені за час t, виконується

$$H_s(t)+H_l(t)=M\left(v_s(t)\right)+M\left(v_l(t)\right)=M\left(v_s(t)+v_l(t)\right)=H(t)=\alpha\lambda t\,, \qquad (6)$$

де $H_s(t)$, $H_l(t)$ — функції відновлення потоку обслужених і потоку втрачених заявок.

Отримано аналітичний вираз для функції відновлення потоку заявок, які обслуговано:

$$H_s(t)=\frac{\alpha\lambda(\lambda+\mu)}{(\alpha+1)\lambda+\mu}t-\frac{\alpha\lambda(\lambda+\mu)}{\left((\alpha+1)\lambda+\mu\right)^2}\left(1-e^{-((\alpha+1)\lambda+\mu)t}\right). \qquad (7)$$

Враховуючи умову (6) і (7), функція відновлення потоку втрачених заявок має вигляд:

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

Імітаційне моделювання

З метою дослідження поведінки функцій відновлення вхідного пуассонівського потоку та потоків обслужених і втрачених заявок для математичної моделі ГРІІБ використано програмну реалізацію імітаційної моделі M/M/1 з втратами (одноканальна СМО з відмовами) та досліджуваної моделі ГРІІБ, тобто M/M/1/0 із підвищенням інтенсивності надходження заявки за умови незайнятості системи (модель СМО з навантаженням). Для здійснення моделювання 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 і сторонніх модулів, серед яких: пакети NumPy, Pandas, бібліотека Matplotlib зі стеку SciPy, Statsmodels тощо [19, 20].

На базі вхідних даних, які враховують певну кратність (рис. 2), роботи моделі ГРІІБ (інтенсивність потоку заявок (інтенсивність надходження заявок)), параметр навантаження (параметр підвищення інтенсивності надходження заявок), продуктивність каналу (сервера) обслуговування заявок (інтенсивність обслуговування заявок) і кількість циклів для проведення сценаріїв експериментів) проводиться розрахунок показників ефективності СМО (рис. 3) (середній час надходження, обслуговування заявки, середній час перебування заявки в системі, частки заявок, які обслуговано і які не обслуговано, в загальній кількості, інтенсивність потоку заявок, які втрачено і обслуговано в граничному випадку).

```
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 ГРІІБ) з підвищенням інтенсивності надходження заявок за умови незайнятості системи

```
Average time of receipt of the request:          0.3333333333333333
Average service time requirements:               0.2857142857142857
Average time spent by a request in the system:   0.15384615384615385
Relative bandwidth:                              0.5384615384615385
Absolute bandwidth:                              1.6153846153846156
The probability that the channel is busy:        0.46153846153846145
The intensity of the flow of lost requirements: 1.3846153846153844
```

Рис. 3. Системні характеристики M/M/1/0 (модель ГРІБ) з підвищенням інтенсивності надходження заявки за умови незайнятості системи

Рис. 4 демонструє поведінку функцій відновлення роботи системи в нормальному режимі. Для системи M/M/1 за відповідних вхідних даних найбільш стрімке відновлення притаманне функції відновлення вхідного потоку, мінімальне спостерігається для функцій відновлення втрачених заявок.

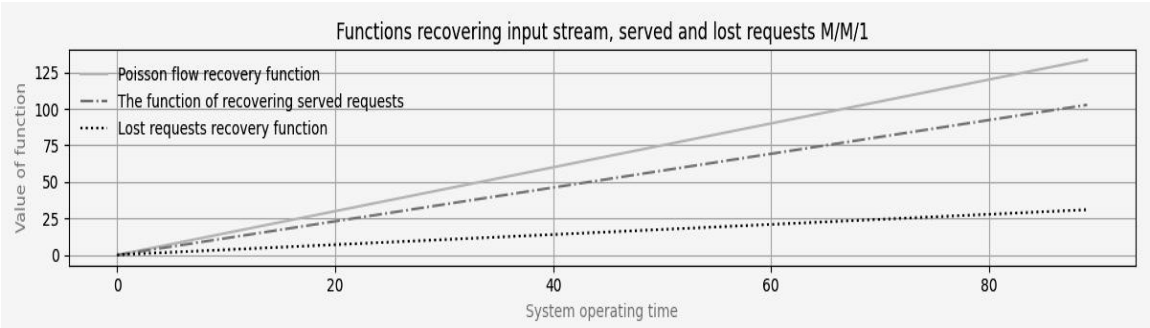

Рис. 4. Графіки функцій відновлення вхідного потоку заявок, які обслуговано та втрачено, для M/M/1 (модель без відновлення)

Рис. 5 демонструє поведінку функцій відновлення роботи системи з навантаженням (ГРІБ з відновленням). Ситуація кардинально змінюється для системи з підвищенням інтенсивності надходження заявки за умови незайнятості системи:

— кутовий коефіцієнт прямої графіка функції відновлення ерлангівського вхідного потоку збільшився на показник параметра підвищення інтенсивності надходження заявок;

— зменшення пропускної спроможності в умовах збільшення навантаження на систему призводить до зміни значень функцій відновлення заявок, які обслуговано та втрачено, з плином часу роботи системи, причому остання функція демонструє активне зростання даних значень.

Варто відмітити, що інтенсивності певних потоків заявок, які обслуговано та втрачено, посилюються майже до лінійного закону, графіки яких теж представлені прямими (рис. 4, 5). Відмітимо, що відповідні функції (7), (8) мають залишкову показникову частину, яка при збільшенні значення t втрачає свій вплив на поведінку функцій.

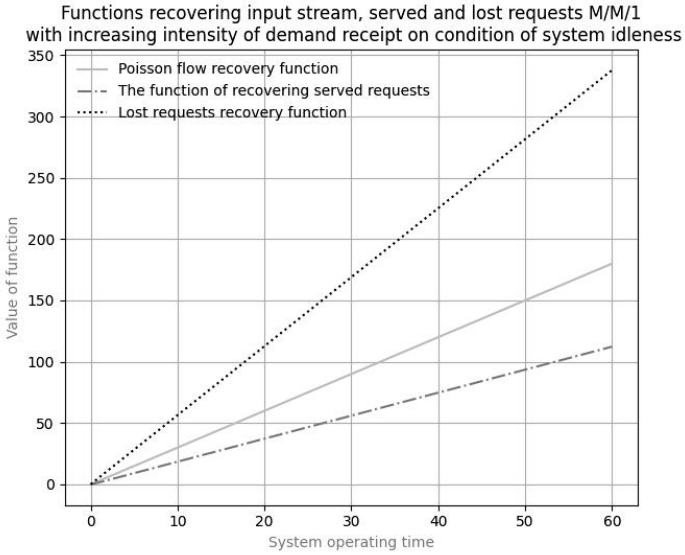

Рис. 5. Графіки функцій відновлення вхідного потоку, заявок, які обслуговано та втрачено, для M/M/1/0 (модель з відновленням) з підвищенням інтенсивності надходження заявки за умови незайнятості системи

Обговорення результатів і перспективи подальших досліджень

Робота ГРІІБ в умовах наростання інтенсивності кібератак з урахуванням необхідності відновлення ефективної роботи спеціалістів має суттєві відмінності від роботи без урахування відновлення. У випадку відсутності відновлення має місце зменшення ефективності роботи внаслідок втрати можливості обробки ряду заявок у процесі протидії кібератакам. Таким чином, за результатами запропонованої моделі для підвищення ефективності ГРІІБ у протидії кібератакам з інтенсивністю, яка наростає, можна запропонувати такий метод.

Етап 1. Здійснюється класифікація існуючих ГРІІБ за характеристиками відновлення їхньої роботи залежно від інтенсивності кібератаки. Такі характеристики будуть залежати не тільки від особливостей сприйняття та обробки інформації спеціалістами ГРІІБ. Вони повинні також враховувати специфічні особливості кожного спеціаліста в рамках можливостей ефективно протидіяти стресовій ситуації, а також особливості, що характеризують відновлення його працездатності. Крім того, важливе значення має розробка орієнтованих на конкретного спеціаліста методів психологічного відновлення його працездатності та наявність можливості застосувати такі методи під час роботи ГРІІБ.

Характеристики відновлення ГРІІБ повинні бути виражені через характеристики запропонованої у роботі моделі.

Етап 2. Розробляються методи ідентифікації поточної інтенсивності кібератаки. Як і на попередньому етапі дані характеристики повинні бути виражені через характеристики моделі, яку описано в роботі.

Етап 3. Виявляються критичні значення характеристик, за яких діяльність ГРІІБ перестає задовольняти заданим умовам ефективності протидії кібератакам із наростаючою інтенсивністю.

Такого характеру значення легко можуть бути виражені через параметри моделі, що запропонована в роботі. Відмітимо, що критичні значення можуть бути також визначені зі спеціальних експериментів. Наприклад, для цього можна використати спеціально організовані навчання та тренування ГРІБ.

Етап 4. Використовуючи результати розробленої моделі, здійснюється моніторинг поточної ефективності роботи даної ГРІБ у процесі протидії кібератакам з урахування підвищення їхньої інтенсивності.

Етап 5. За умови, коли діяльність ГРІБ досягає критичних значень параметрів ефективності, здійснюється прийняття рішення або про продовження роботи даної ГРІБ, або про залучення нової ГРІБ (уже з тими параметрами, які будуть задовольняти заданому рівню ефективності протидії) для продовження реалізації протидії кібератакам. Можливий також варіант розгляду залучення до ГРІБ додаткових спеціалістів для того, щоб після такого оновлення ГРІБ змогла продовжити ефективно протидіяти кібератакам. Також можна запропонувати заміну деяких спеціалістів, щоб у результаті характеристики отриманої нової ГРІБ дозволили ефективно протидіяти кібератакам.

Використання описаного методу вимагає проведення спеціально організованого комплексу тренувань, які можуть бути опрацьовані з урахуванням результатів запропонованої моделі. При цьому потрібно врахувати не тільки характеристики кожного спеціаліста зі складу даної ГРІБ. Потрібно також врахувати, що характеристики спільної роботи колективу спеціалістів часто не є адитивними. Тому виникає потреба досліджувати ГРІБ із різним складом персоналу.

У цілому, отримані в роботі результати дозволяють розробити систему заходів, яка дозволить суттєво підвищити ефективність діяльності щодо протидії кібератакам із наростанням інтенсивності за допомогою управління кадровим складом ГРІБ і використанням груп із достатньою для протидії ефективністю.

Висновки

Побудовано модель для розрахунку ефективності діяльності ГРІБ з відновленням в умовах протидії кібератакам із підвищенням їхньої інтенсивності. Отримано функцію відновлення пуассонівського потоку та щільність її відновлення, запропоновано формули для функцій відновлення потоку заявок, які обслуговано та втрачено, для процесу відновлення ГРІБ під час кібератаки.

Досліджено поведінку функцій відновлення вхідного пуассонівського потоку та потоків заявок, які обслуговано та втрачено, математичної досліджуваної моделі ГРІБ в умовах навантаження. Особливість побудованої моделі полягає в урахуванні параметра підвищення інтенсивності ідентифікації подій інформаційної безпеки.

Проведено імітаційне моделювання діяльності ГРІБ, яке показало, що можна спрогнозувати показники зміни ефективності їхньої діяльності в процесі протидії кібератакам із наростанням інтенсивності.

Розроблений математичний апарат призначений для застосування при постановці та вирішенні різних оптимізаційних завдань під час роботи ГРІБ, яка передбачає блокування кібератаки, ліквідацію її наслідків, розробку заходів з мінімі-

зації ризиків виникнення в майбутньому подібних інцидентів за умови випадкового характеру генерування подій інформаційної безпеки.

1. Eltantawy N., Wiest J. The Arab Spring. Social Media in the Egyptian Revolution: Reconsidering resource mobilization theory. *Int. J. Commun*. 2011. Vol. 5. P. 1207–1224.

2. Wolfsfeld G, Segev E, Sheafer T. Social media and the Arab Spring: Politics comes first. *Int. J. Press/Politics*. 2013. V. 18. P. 115–137.

3. Del Vicario M., Bessi A., Zollo F., et al. The spreading of misinformation online. *Proceedings of the National Academy of Sciences*. 2016. Vol. 113(3). P. 554–559.

4. Shao C., Ciampaglia G.L., Varol O., et al. The spread of low-credibility content by social bots. Nat Commun. 2018. Vol. 9. Article 4787. URL: https://doi.org/10.1038/s41467-018-06930-7

5. Bail C.A., Argyle L.P., Brown T.W., et al. Exposure to opposing views on social media can increase political polarization. *Proceedings of the National Academy of Sciences*. 2018. Vol. 115(37). P. 9216–9221.

6. Ross B., Pilz L., Cabrera B. et al. Are social bots a real threat? An agent-based model of the spiral of silence to analyse the impact of manipulative actors in social networks. *European Journal of Information Systems*. 2019. Vol. 28(4). P. 394–412.

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

8. Grispos G., Glisson W., Storer T. How Good is Your Data? Investigating the Quality of Data Generated During Security Incident Response Investigations. Proceedings of the 52nd Hawaii International Conference on System Sciences. Hawaii International Conference on System Sciences, 2019. P. 7156–7165. URL: https://doi.org/10.24251/hicss.2019.859

9. Camacho J., García-Giménez J. M., Fuentes-García N. M., Maciá-Fernández G. Multivariate Big Data Analysis for Intrusion Detection: 5 steps from the haystack to the needle. *Computers & Security*. 2019. Vol. 87. Article 101603. URL: https://doi.org/10.1016/j.cose.2019.101603.

10. Nyre-Yu M., Gutzwiller R.S., Caldwell B.S. Observing Cyber Security Incident Response: Qualitative Themes from Field Research. Proceedings of the Human Factors and Ergonomics Society Annual Meeting: SAGE Publications Sage CA: Los Angeles, CA, 2019. P 437–441.

11. Phuong P., Vivek J., Dauterman L., Ormont J., Navendu J. DeepTriage: Automated Transfer Assistance for Incidents in Cloud Services. KDD'20: Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. Virtual Event CA USA, 2020. P. 3281–3289.

12. Ahmad A., Desouza K.C., Maynard S.B., et al. How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*. 2020. Vol. 71(8). P. 939–953.

13. Котик М.А., Емельянов А.М. Природа ошибок человека-оператора. Москва: Транспорт, 1993. 252 с.

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

15. Вудсон У., Коновер Д. Справочник по инженерной психологии для инженеров и художников-конструкторов. Москва: МИР, 1968. 520 с.

16. Маталыцкий М., Хацкевич Г. Теория вероятности и математическая статистика. Москва: ЛитРес, 2021. 350 с.

17. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и её инженерные приложения. Москва: Наука, 1991. 384 с.

18. Каштанов В.А, Медведев А.И. Теория надежности сложных систем. Москва: ФИЗМАЛИТ, 2010. 608 с.

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

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

Надійшла до редакції 10.11.2021