УДК 614.8 **doi: 10.26906/SUNZ.2021.1.119**

М. Д. Кацман[1], В. І. Мацюк[2], П. В. Лапін[1]

[1] Акціонерне товариство «Українська залізниця», Київ, Україна
[2] Державний університет інфраструктури і технологій, Київ, Україна

МАТЕМАТИЧНА МОДЕЛЬ ОХОРОНИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Мета роботи – побудова математичної моделі, яка описує характеристики захисту об'єктів критичної інфраструктури, пов'язаної з роботою охоронної групи. **Результати.** В статті розглянуті деякі поширені математичні моделі протидії тероризму та актам незаконного втручання на об'єкти критичної інфраструктури. Авторами запропоновано використання методів теорії масового обслуговування марківського і немарківського типів задля моделювання протидії персоналом охорони зловмисним угрупованням з випадковим числом зловмисників у групі та різними способами організації дій такого персоналу. Модель охорони об'єкту критичної інфраструктури розглядається як система масового обслуговування (СМО), яка складається із СМО першої і другої груп моделює ешелоновану протидію групам зловмисників. Наведено диференційні рівняння Колмогорова для імовірностей станів цієї СМО. **Висновки.** Використання запропонованих моделей захисту об'єктів критичної інфраструктури від актів несанкціонованого втручання дозволить визначити раціональні значення співвідношень величин кількісного складу підрозділів охорони, інтенсивностей застосування засобів протидії і зосередження додаткових сил і засобів охорони з інтенсивністю проникнення на об'єкт зловмисних угруповань з випадковим числом зловмисників у групі задля забезпечення прийнятної імовірності виявлення, запобігання і нейтралізації таких угруповань.

Ключові слова: об'єкт охорони, система масового обслуговування, неординарний потік груп зловмисників, випадкове число зловмисників у групі, СМО немарківського типу, персонал охорони

Вступ

Проблемі протидії тероризму та актам незаконного втручання у діяльність об'єктів критичної інфраструктури нині присвячено багато наукових робіт. Класифікація моделей протидії тероризму знайшла своє відображення у роботі [1], в якій приведений огляд сучасних робіт щодо моделювання системи протидії тероризму, запропонована класифікація моделей тероризму та моделей протидії тероризму. До концептуальних моделей у цій роботі пропонується віднести моделі, які розробляються спеціалістами предметної області, політологами, психологами, соціологами. Як приклад, наводиться робота [2], в якій подані емпіричні дані щодо моделей прийняття рішень учасниками терористичних організацій на різних рівнях: стратегічному, тактичному та оперативному, а також на рівні окремого терориста.

Моделі аналізу і синтезу, як правило, є математичними чи фізичними моделями. В огляді [3] охарактеризовано і наведено більше таких робіт. Зокрема у роботі [4] розроблена основа для розвитку класифікації терористичних угруповань хімічної, біологічної, радіологічної та ядерної зброї з використанням евристичного методу розпізнавання образів, методу дерев класифікації і дискримінаційного аналізу. Стосовно систем безпеки на транспорті ряд робіт присвячений аналізу пристроїв задля підвищення імовірності виявлення і зниження інтенсивності помилкових тривог. У роботі [5] з використанням байєсовського аналізу наведений метод ранжирування загроз і визначення пріоритетів заходам безпеки об'єктам.

Складність реальних ситуацій, пов'язаних із забезпеченням безпеки, потребують універсальності застосованих математичних моделей.

Ці вимоги неминуче приводять у протиріччя із спільністю та обґрунтованістю результатів моделювання, тому при розв'язуванні моделей у вигляді ієрархії (звичайно більш низьким рівням ієрархії відповідає більш висока ступінь деталізації опису модельованих систем) або горизонтальному ланцюжку, у кожному елементі якого ступінь деталізації приблизно однаковий [6].

В роботі [1] детально розглянуті рівня моделювання (ієрархії моделей) протидії тероризму. Теоріко-ігрові моделі боротьби з тероризмом подані у роботах [7,8,9]. В роботі [10] запропонований підхід до створення математичної моделі функціонування систем фізичного захисту об'єктів як процесу взаємодії множин на основі теорії звичайних множин, теорії нечітких множин і методу аналізу ієрархій.

В роботі [11] запропонована математична модель опису характеру взаємодії між складовими системи «захисник – зловмисник» як складовими системи «хижак – жертва». Модель являє собою модифіковану класичну модель конкуренції Лоткі – Вольтерри, яка дозволяє оцінювати зміни рівня небезпеки об'єкта із зміною його захищеності.

Застосування нечіткого когнітивного моделювання задля попередження ризикових ситуацій в умовах нечітких вихідних даних на об'єктах критичних інфраструктур розглядається в роботі [12]. В ній пропонується управлінська структура АЕС у вигляді нечіткої когнітивної моделі, приведені сценарії ризикових ситуацій і наведений їхній аналіз.

В роботі [13] розглянуті можливості застосування моделей і методів дослідження операцій для планування захисту об'єктів критичної інфраструктури. Адаптація цих моделей включає врахування стохастичної, інформаційної і поведінкової невизначеностей терористів. У цій роботі, зокрема, розглянуті узагальнення задач антагоністичної гри нападу

і захисту та оптимального розподілу захисних ресурсів.

Прикладом використання комплексних моделей з параметрами, обмірюваними у різних шкалах, є теоретико-ігрова модель для забезпечення безпеки у міжнародному аеропорту у м. Лос-Анджелес, на основі якої розроблена і введена в експлуатацію автоматизована система «Помічник для рандомізованого контролю маршрутів» (ARMOR) [14].

У роботі [15] представлений опис тестів для перевірки ARMOR, який експлуатується з 2007 р.

Таким чином, задля моделювання систем фізичної охорони об'єктів застосовується широкий спектр математичних моделей.

На наш погляд, з метою визначення ефективності дій підрозділу охорони об'єктів критичної інфраструктури, доцільно застосовувати математичний апарат теорії масового обслуговування.

Результати досліджень

Розглянемо об'єкт, що охороняється підрозділом охорони з n осіб, як систему масового обслуговування. На об'єкт намагаються проникнути групи зловмисників з інтенсивністю λ з метою створення загрози його безпечного функціонування. Взагалі чисельність групи зловмисників може бути випадковим, іншими словами з імовірністю a_s група може складатися з *s* зловмисників.

Тобто на n-канальну СМО надходить потік λ [груп/од.часу] групових заявок з випадковим числом заявок у групі.

Подібні СМО знайшли своє застосування у математичних моделях інформаційних технологій, що знайшло своє відображення у роботах [16-18].

Однією з особливостей СМО, що розглядається, є те, що час $\bar{t}_{зл.}$ перебування зловмисників на об'єкті є обмеженим, воно є випадковою величиною, яке підпорядковане показовому закону з параметром $\eta = 1/\bar{t}_{зл.}$.

Параметр η є інтенсивністю покидання заявок із канала обслуговування СМО внаслідок обмеження їхнього перебування в системі.

Параметр μ характеризує систему протидії $\mu = 1/\bar{t}_{ox}$ [зловм/од.часу], де $\bar{t}_{ox}$ - середній час застосування охоронником засобів протидії зловмиснику.

Протидія зловмисникам з боку підрозділу охорони може бути організована різними способами, що обумовлює тип системи масового обслуговування. До першої групи СМО належать:

1. СМО M/M/n/m з обмеженням ($\eta \neq 0$), без взаємодопомоги ($h = n$, $g = 1$), неординарними заявками і випадковим числом заявок у групі. Тут *h* величина, що дорівнює відношенню всієї кількості *n* охоронників (каналів обслуговування) до кількості *g* охоронників, які об'єднані у групу протидії одному зловмиснику, тобто $n = n/g$.

2. СМО M/M/n/m з обмеженням ($\eta \neq 0$), повною взаємодопомогою (h =1; g = n), неординарними заявками і випадковим числом заявок у групі.

3. СМО M/M/n/m з обмеженням ($\eta \neq 0$), з частковою взаємодопомогою ($h = n/g$), неординарними заявками і випадковим числом заявок у групі.

До другої групи належать СМО немарковського типу, які моделюють умови, коли сили і засоби охорони не знаходяться на об'єкті, наприклад, коли необхідно зосередити додаткові сили і засоби. Тобто процес протидії складається з двох фаз тривалістю відповідно $\bar{t}_1$ - часу зосередження і $\bar{t}_{ox}$ - часу застосування засобів протидії, де $\bar{t}_1$, має показове розподілення з параметром $\mu_1 = 1/\bar{t}_1$. [охор./од. часу], а $\bar{t}_2$ – з параметром $\mu_2 = 1/\bar{t}_{ox}$ [зловм./од. часу]. Тобто сумарний час протидії має узагальнене розподілення Ерланга з параметрами μ_1 і μ_2.

Такі СМО мають обмеження ($\eta \neq 0$), можуть бути з різними характеристиками взаємодопомоги, є система масового обслуговування з неоднорідними заявками і випадковим числом заявок у групі.

Деякі аспекти математичних моделей цих СМО розглянуті у роботах [19-22].

Розглянемо більш детально СМО 1-ої групи.

1.1 СМО M/M/n/m з обмеженням ($\eta \neq 0$), без взаємодопомоги (h = n, g = 1), неординарними заявками і випадковим числом заявок у групі.

Диференціальні рівняння Колмогорова для імовірностей станів цієї СМО:

$$\frac{dP_0(t)}{dt} = -\lambda P_0(t) + (\mu + \eta) P_1(t);$$

$$\frac{dP_0}{dt} = -(\lambda + \mu + \eta) P_1(t) + \lambda a_1 P_0(t) + 2(\mu + \eta) P_2(t);$$

$$\frac{dP_2(t)}{dt} = -(\lambda + 2\mu + 2\eta) P_2(t) + \\ + \lambda \sum_{s=1}^{2} s a_s P_{2-s}(t) + 3(\mu + \eta) P_2(t);$$

……

$$\frac{dP_k(t)}{dt} = -(\lambda + k\mu + k\eta) P_k(t) + \lambda P_{k+1}(t) \times \\ \times \sum_{s=1}^{k} s a_s P_{k-s}(k+1)(\mu + \eta) \text{ при } 1 \le k < n;$$

……

$$\frac{dP_k(t)}{dt} = -(\lambda + n\mu + k\eta) P_k(t) + \lambda \sum_{s=1}^{n} s a_s P(t)_{n-s}(t) + \\ + [n\mu + (k+1)\eta] P_{k+1}(t) \quad при \; k \ge n.$$

1.2. СМО M/M/n/m з обмеженням ($\eta \neq 0$), повною взаємодією ($h = 1$, $g = n$), неординарними заявками і випадковим числом заявок у групі.

Особливостями функціонування цієї СМО, а отже , організації протидії є:

- перша заявка обслуговується усіма каналами обслуговування з інтенсивністю μ= nμ+η;

- наступна заявка обслуговується частиною каналів обслуговування, інші продовжують обслуговування попередньої заявки, якщо воно не було закінчене;

- після закінчення обслуговування будь=якої заявки, група каналів, яка звільнилася, під'єднується до обслуговування заявок, які є в системі;

- у марківській (пуассонівській) СМО характеристики обслуговування не залежать від розподілення каналів між заявками, лише воно було би рівномірним й усі канали брали би участь в обслуговуванні одночасно [20];

- якщо в системі вже є n заявок, то (n+1)-а заявка стає у чергу.

Система диференціальних рівнянь імовірностей станів має вигляд:

$$\frac{dP_0(t)}{dt} = -\lambda P_0(t) + \mu^* P_1(t);$$

$$\frac{dP_1(t)}{dt} = -(\lambda + \mu^*)P_1(t) + \lambda a_1 P_0(t) + 2\mu^* P_2(t);$$

$$\frac{dP_2(t)}{dt} = -(\lambda + 2\mu^*)P_2(t) + \lambda\sum_{s=1}^{2} sa_s P_{2-s}(t) + 3\mu^* P_3(t);$$

……

$$\frac{dP_k(t)}{dt} = -(\lambda + k\mu^*)P_k(t) + \lambda\sum_{s=1}^{k} sa_s P_{k-s}(t) + (k+1)\mu^* P_{k+1}(t) \text{ при } 1 \le k < n;$$

……

$$\frac{dP_k(t)}{dt} = -(\lambda + n\mu^* + k\eta)P_k(t) + \lambda\sum_{s=1}^{n} sa_s P_{n-s}(t) + [n\mu^* + (k+1)\eta]P_{k+1}(t) \text{ при } k \ge n.$$

1.3. СМО M/M/n/m з обмеженням ($\eta \neq 0$), частковою взаємодією (h = n/g), неординарними заявками і випадковим числом заявок у групі.

Система диференціальних рівнянь імовірностей станів системи буде такою:

$$\frac{dP_0(t)}{dt} = -\lambda P_0(t) + \mu_g^* P_1(t);$$

$$\mu_g^* = g\mu + \eta;$$

$$\frac{dP_1(t)}{dt} = -(\lambda + \mu_g^*)P_1(t) + \lambda a_1 P_0(t) + 2\mu_g^* P_2(t);$$

$$\frac{dP_2(t)}{dt} = -(\lambda + 2\mu_g^*)P_2(t) + \lambda\sum_{s=1}^{2} sa_s P_{2-s}(t) + 3(\mu_g^* P_3(t);$$

……

$$\frac{dP_i(t)}{dt} = -(\lambda + i\mu_g^*)P_i(t) + \lambda\sum_{s=1}^{i} sa_s P_{i-s}(t) + (i+1)\mu_g^* P_{i+1}(t) \text{ при } 0 < i < h;$$

……

$$\frac{dP_h(t)}{dt} = -(\lambda + n\mu_g^*)P_h(t) + \lambda\sum_{s=1}^{h} sa_s P_{h-s}(t) + (n\mu + (h+1)\eta)P_{h+1}(t);$$

$$\frac{dP_{h+1}(t)}{dt} = -(\lambda + h\mu_g^* + \eta)P_{h+1}(t) + \lambda \times \times\sum_{s=1}^{h+1} sa_s P_{(h+1)-s}(t) + (h\mu_g^* + 2\eta)P_{h+2}(t);$$

……

$$\frac{dP_j(t)}{dt} = -(\lambda + h\mu_g^*(j-h)\eta)P_j(t) + \lambda\sum_{s=1}^{j} sa_s P_{j-s}(t) + (h\mu_g^* + (j-h+1)\eta) \times \times P_{j+1}(t) \text{ при } h < j < n;$$

……

$$\frac{dP_k(t)}{dt} = -(\lambda + n\mu_g^*)P_n(t) + \lambda\sum_{s=1}^{k} sa_s P_{n-s}(t) + (n\mu_g^* + \eta)P_{n+1}(t) \text{ при } k \ge n.$$

Імовірність проникнення зловмисників на об'єкт з причини того, що охорона не встигає протидіяти зловмисникам можно обчислити з формули:

$$P_{зн} = \eta\sum_{k=1}^{\infty} kP_k \Big/ \left(\lambda\sum_{k=1}^{\infty} ka_k\right). \qquad (1)$$

Імовірність того, що зловмисники будуть нейтралізовані буде:

$$P_{нейтр} = 1 - P_{зн}. \qquad (2)$$

СМО другої групи розглянемо на прикладі системи масового обслуговування $M/E_2/n/m$ з обмеженням ($\eta \neq 0$), без взаємодопомоги, з неординарними заявками і випадковим числом заявок у групі.

Система диференціальних рівнянь імовірностей станів цієї СМО має вигляд:

$$\frac{dP_{00}(t)}{dt} = -\lambda P_{00}(t) + \mu_2^* P_{21}(t);$$

$$\frac{dP_{11}(t)}{dt} = -(\lambda + \mu_1^*)P_{11}(t) + \lambda a_1 P_{00}(t) + 2\mu_2^* P_{22}(t);$$

$$\frac{dP_{21}(t)}{dt} = -(\lambda + \mu_2^*)P_{21}(t) + \mu_1^* P_{11}(t);$$

$$\frac{dP_{12}(t)}{dt} = -(\lambda + 2\mu_1^*)P_{12}(t) + \lambda a_1 P_{11}(t) + 2\lambda a_2 P_{00}(t) + 3\mu_2^* P_{23}(t) + \lambda P_{21}(t);$$

$$\frac{dP_{22}(t)}{dt} = -(\lambda + 2\mu_2^*)P_{22}(t) + 2\mu_1^* P_{12}(t);$$

……..……..……

$$\frac{dP_{1k}(t)}{dt} = -(\lambda + k\mu_1^*)P_{1k}(t) + \lambda\sum_{s=1}^{k} sa_s P_{1(k-s)}(t) +$$
$$+[(k+1)\mu_2^* + \eta]P_{2(k+1)}(t) +$$
$$+\lambda P_{2(k-1)}(t) \text{ при } k < n;$$

$$\frac{dP_{2k}(t)}{dt} = -(\lambda + k\mu_2^*)P_{2k}(t) +$$
$$+k\mu_1^* P_{1k}(t) \text{ при } k < n;$$

……..……..……

$$\frac{dP_{1k}(t)}{dt} = -(\lambda + \eta\mu_1^* + k\eta)P_{1k}(t) + \lambda\sum_{s=1}^{k} sa_s P_{1(k-s)}(t) +$$
$$+\lambda P_{2(k-1)}(t) + (\eta\mu_2^* + k\eta)P_{2(k+1)} \text{ при } k > n;$$

$$\frac{dP_{2k}(t)}{dt} = -(\lambda + n\mu_2^* + k\eta)P_{2k}(t) +$$
$$+(n\mu_1^* + k\eta)P_{1k}(t) \text{ при } k > n.$$

Математична модель СМО $M/E_2/n/m$ детально розглянута у [22]. Система масового обслуговування, яка складається із СМО першої і другої груп моделює ешелонову протидію групам зловмисників (рис. 1). Імовірності проникнення і нейтралізації зловмисників можна обчислити з формул (1) і (2).

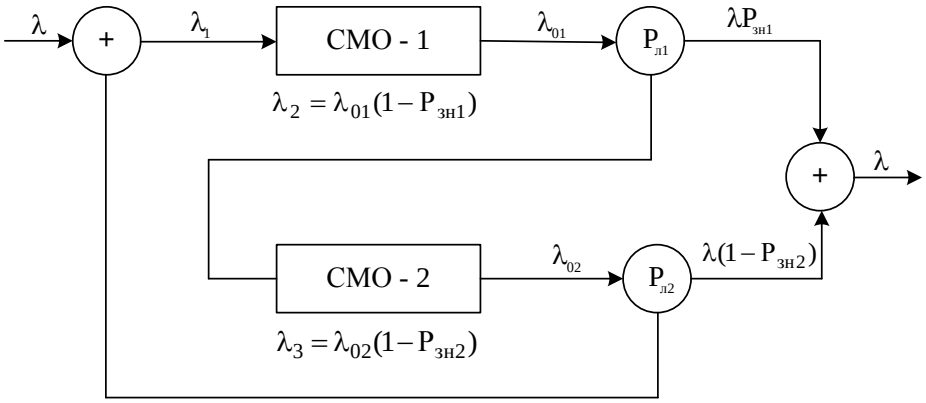

Рис. 1. СМО ешелованої протидії

У стаціонарному режимі буде мати місце такі рівняння:

$$\lambda_1 = \lambda_{01};\ \lambda_2 = \lambda_{02};$$
$$\lambda_2 = \lambda_{01}(1 - P_{зн1}) = \lambda(1 - P_{зн1}) = \lambda P_{прон1};$$
$$\lambda_{01} = \lambda_{01}(1 - P_{зн1})\cdot P_{зл2}^{-1} = \lambda P_{прон1}\cdot P_{л2}^{-1};$$
$$\lambda_2 = \lambda_{02}(1 - P_{зн2}) = \lambda(1 - P_{зн1})(1 - P_{зн2})\cdot P_{зн2}^{-1} =$$
$$= \lambda P_{прон1}\cdot \lambda P_{прон2}\cdot P_{зн2}^{-1}.$$

Умови стаціонарної роботи СМО:

$$\omega_1 = \frac{\lambda}{n_1(\mu_1 + \eta_1)} < 1;$$

$$\omega_2 = \frac{\lambda P_{прон1}}{n_2(\mu_2 + \eta_2)} < 1.$$

Повне математичне сподівання часу перебування заявки у СМО:

$$\bar{t} = (\bar{t}_{смо1} + \bar{t}_{смо2})P_{зн2}^{-1}.$$

Розглянемо приклад.

На об'єкт, що охороняється підрозділом охорони у складі трьох осіб (n = 3) здійснюється напад групи зловмисників з інтенсивністю λ = 1 [гр/од.часу]. У кожній групі з імовірністю a_s може бути різна кількість зловмисників. Закон розподілу числа зловмисників у групі рівномірний, тобто з імовірністю 0,2 у групі можуть бути 1,2,3,4 чи 5 зловмисників: $a_1 = a_2 = a_3 = a_4 = a_5 = 0{,}2$. Час перебування зловмисників на об'єкті $\bar{t}_{зл}$ є обмеженою випадковою величиною яка підпорядкована по показовому закону з параметром $\eta = 1/\bar{t}_{зл}$. Інтенсивність протидії осіб охорони $\mu = 1/\bar{t}_{ox}$ [зловмисників/од.часу]. Необхідно визначити імовірність нейтралізації зловмисників охороною об'єкта при різних співвідношеннях λ:μ:η.

На рис 2 представлена СМО охорони об'єкта для приклада, що розглядається.

Диференційні рівняння Колмогорова для імовірностей станів цієї СМО будуть:

$$\frac{dP_1(t)}{dt} = -\lambda P_0(t) + \mu^* P_1(t);$$

$$\frac{dP_1(t)}{dt} = -(\lambda + \mu^*)P_1(t) + \lambda a_1 P_0(t) + 2\mu^* P_2(t);$$

$$\frac{dP_2(t)}{dt} = -(\lambda + 2\mu + 2\eta)P_2(t) + \lambda a_1 P_1(t) +$$
$$+2\lambda a_2 P_0(t) + 3\mu^* P_3(t);$$

$$\frac{dP_3(t)}{dt} = -(\lambda + 3\mu + 3\eta)P_3(t) + \lambda a_1 P_2(t) +$$
$$+2\lambda a_2 P_1(t) + +3\lambda a_3 P_1(t) +$$
$$+3\lambda a_3 P_0(t) + (3\mu + 4\eta)P_4(t);$$

$$\frac{dP_4(t)}{dt} = -(\lambda + 3\mu + 4\eta)P_4(t) + \lambda a_1 P_3(t) + \\ +2\lambda a_2 P_2(t) + 3\lambda a_3 P_1(t) + \\ +4\lambda a_4 P_0(t) + (3\mu + 5\eta)P_5(t);$$

$$\frac{dP_5(t)}{dt} = -(\lambda + 3\mu + 5\eta)P_5 + \lambda a_1 P_4(t) + 2\lambda a_2 \times \\ \times P_3(t) + 3\lambda a_3 P_2(t) + 4\lambda a_4 P_1(t) + \\ +5\lambda a_5 P_0(t) + (3\mu + 6\eta)P_6(t).$$

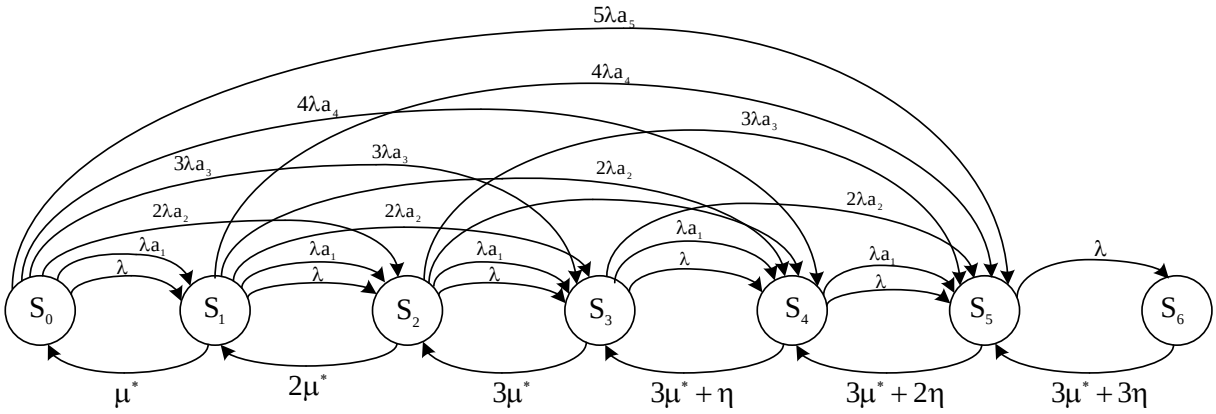

Рис. 2. СМО охорони об'єкта для прикладу, що розглядається

Нормуюча умова:

$$\sum_{k=0}^{6} = 1;$$

$\mu^* = \mu + \eta$.

Для стаціонарних умов функціонування цієї СМО лінійні рівняння мають вигляд

$$0 = -\lambda P_0(t) + \mu^* P_1;$$

$$0 = -(\lambda + \mu^*)P_1 + \lambda a_1 P_0 + 2\mu^* P_2;$$

$$0 = -(\lambda + 2\mu^*)P_2 + \lambda a_1 P_1 + 2\lambda a_2 P_0 + 3\mu^* P_3$$

$$0 = -(\lambda + 3\mu^*)P_3 + \lambda a_1 P_2 + 2\lambda a_2 P_1 + 3\lambda a_3 P_1 + \\ +3\lambda a_3 P_0 + (3\mu^* + \eta)P_4;$$

$$0 = -(\lambda + 3\mu^* + \eta)P_4 + \lambda a_1 P_3 + 2\lambda a_2 P_2 + \\ +3\lambda a_3 P_1 + 4\lambda a_4 P_0 + (3\mu^* + 2\eta)P_5;$$

$$0 = -(\lambda + 3\mu^* + 2\eta)P_5 + \lambda a_1 P_4 + 2\lambda a_2 P_3 + \\ +3\lambda a_3 P_2 + 4\lambda a_4 P_1 + 5\lambda a_5 P_0 + (3\mu^* + 3\eta)P_6;$$

Імовірність $P_{нейтр}$ визначалась з формул (5,6).

На рис. 3 поданий графік залежності імовірності $P_{зн}$ при різних значеннях μ та η.

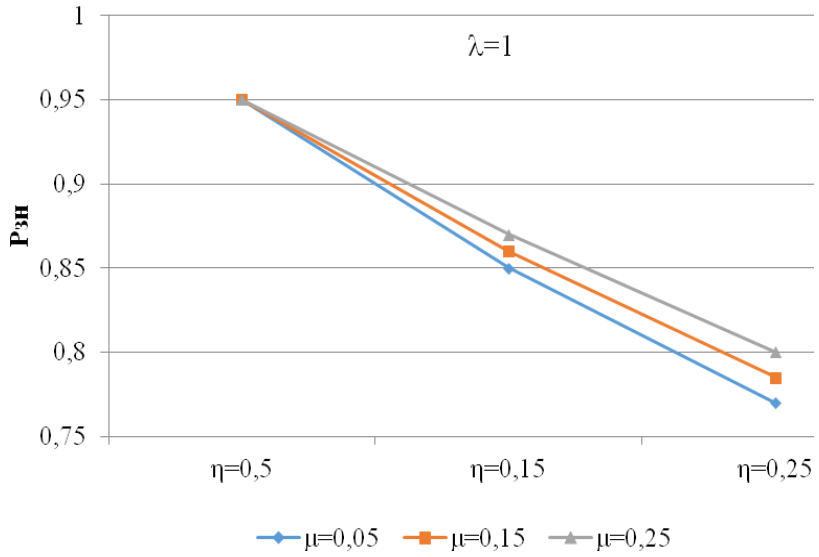

Рис. 3. Графік залежності імовірності нейтралізації зловмисників від величини інтенсивностей протидії

З рис. 3 видно, що із збільшенням інтенсивності протидії величина імовірності $P_{зн}$ збільшується навіть при зменшенні часу перебування зловмисників на об'єкті охорони.

Висновок

Використання запропонованих моделей захисту об'єктів критичної інфраструктури від актів

несанкціонованого втручання дозволить визначити раціональні значення співвідношень величин кількісного складу підрозділів охорони, інтенсивностей застосування засобів протидії і зосередження додаткових сил і засобів охорони з інтенсивністю проникнення на об’єкт зловмисних угруповань з випадковим числом зловмисників у групі задля забезпечення прийнятної імовірності виявлення, запобігання і нейтралізації таких угруповань.

СПИСОК ЛІТЕРАТУРИ

1. Шумов В.В. Модели протидії тероризму: класифікація. Труди ИСА РАН. Том 62, 3/2012, С.106-115.
2. Social Science for Counterterrorism. Putting the Pieces Together/Davis P.K., Cragin K., Editors. RAND Corporation, 2009.
3. Wright P.D, Liberatore M.I., Nydick R.L, A Survey of Operations Reserch Models and Application in Homeland Security/Interfaces, 2006.V.36, №6, pp.514-529.
4. Sullivan T.J., Perry W.L. Identifying indicators of chemical, biological, radiological and nuclear (CBRN) Weapons development activity in sub-national terrorist group/ J. Oper. Res. Soc. 2004, N 55 (4) , PP. 361-374.
5. Pate-Cornell E. Fusion of intelligence information: A.Bayesian approach/ Risk Anal. 2002, N 22(3), pp. 445-454.
6. Новиков Д.А. Иерархические модели военных действий/ Управление большими системами. Вып. 37.М.:ИПУ РАН, 2012, С.25-62.
7. Bachrach Y., Draief V., Goyal S. Security games with contagion/University of Cambridge, 2011.
8. Bier V., Oliveros S., Samuelson L. Choosing what to protect: Strategic defensive allocation against an unknown attacker//Journal of Public Economic Theory, 2006,N9, pp. 1-25/
9. Kiekintveld C., Tambe M., Marecki J. Robust Bayesian Methods for Stackelberg Security Games//Conference: Autonomous Agents & Multiage Systems/Agent Theories, Architectures and Languages – ATAL, pp. 1467-1468, 2010.
10. Боровский А.С., Тарасов А.Д. Интегрированный подход к разработке общей модели функционирования систем физической защиты объектов // Труды ИСА РАН. Том 61. 1/2011, С. 3-13.
11. Дормидонтов А.В., Миронова Л.В., Миронов В.С. О возможности применения модели противодействия к оценке уровня безопасности объектов транспортной инфраструктуры// Научный Вестник МГТУ. Том 21, № 03, 2018, С.67-77.
12. Гинис Л.А., Колоденкова А.Е. Нечеткое моделирование для предупреждения рисковый ситуаций на объектах критических инфраструктур// Вестник УГАТУ, Том 21, № 4(78), 2017, С. 113-1120.
13. Норкин В.И., Гайворонский А.А., Заславский В.А., Кнопов П.С. Модели оптимального распределения ресурсов для защиты объектов критической инфраструктуры/ Кибернетика и системный анализ. Том 54 № 5, 2018, С.13-26.
14. Pita J., Jain M., Western C., Portway C., Tambe M., Ordonez F., Kraus S., Paruchuri P. Deployed ARMOR protection: The application of a games theoretic model for security at the Los Angeles International Airport/In Proc. Of AAMAS, 2008.
15. Taylor M.E., Kiekintveld C., Western C., Tambe M. Beyond Runtimes and Optimality: Challenges and Opportunities in Evaluating Deployed Security Sistems/ In Proceeding of the AAMAS – 09 Workshop on Agent Design: Advancing from Practice to Theory, May 2009.
16. Рыжков Ю.И. Имитационное моделирование. Теория и технология. СПб: КОРОНА принт, 2004, 384 с.
17. Рыжиков Ю.И. Расчет систем обслуживания с групповыми поступлением заявок/ Информационно-управляющие системы № 2. 2007, С.39-49.
18. Монсик В.Б. , Скрыпников А.А., Федотов А.Ю. Системы массового обслуживания неделимых групповых заявок с очередью неограниченной длины/ Научный Вестник МГТУ ГА № 184, 2012, С. 108-112.
19. Гнеденко Б.В., Коваленко И.Н. Введение в ТМО. – М.: Наука, 1987. – 336 с.
20. Шуенкин В.А., Донченко В.С. Прикладные модели ТМО. К.: НМКВО, 1992, 398 с.
21. Венцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. – Уч. Пособие для втузов – 2-е изд., М.: Высшая школа, 2000. — 383 с.
22. Katsman M. D., Mathematical models of ecologically hazardous rail. Trafficaccidents / M. D. Katsman, V. K., Myronenko, V. I. Matsiuk // Reliability: theory&applications. – Vol. 10, № 1(36). – San Diego, USA – 2015. – P. 28–39.

Received (Надійшла) 22.01.2021
Accepted for publication (Прийнята до друку) 14.04.2021

Mathematical model of critical infrastructure protection

M. Katsman, V. Matsyuk, P. Lapin

Abstract. The purpose of the work is to build a mathematical model that describes the characteristics of the protection of critical infrastructure related to the work of the security team. Results. The article discusses some common mathematical models of counter-terrorism and acts of illegal interference with critical infrastructure. The authors propose the use of methods of queuing theory of Markov and non-Markov types to model the resistance of security personnel to a malicious group with a random number of criminals in the group and different ways of organizing the actions of such personnel. The critical infrastructure protection model is considered as a queuing system (QMS), which consists of QMS of the first and second groups simulates echelon resistance to groups of attackers. Kolmogorov's differential equations for the probabilities of the states of this QMS are given. Conclusions. The use of the proposed models of protection of critical infrastructure from acts of unauthorized interference will determine the rational values of the ratios of the quantitative composition of security units, the intensity of countermeasures and concentration of additional forces and security with the intensity of penetration of malicious groups with a random number of attackers. to ensure an acceptable probability of detection, prevention and neutralization of such groups.

Keywords: security object, queuing system (QS), nonordinary stream of malefactor groups, random number of malefactors in the group, non-Markov type QS, security personnel.