УДК 621.38.044
С.В. Толюпа, В.А. Дружинін
Державний Університет інформаційно-комунікаційних технологій
вул. Солом'янська, 7, 03110, Київ, Україна

ВИКОРИСТАННЯ ТЕОРІЇ ІГОР ДЛЯ РІШЕННЯ ЗАДАЧ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Методи теорії ігор уже зайняли визначене місце в сучасних інформаційних системах. Використання теорії ігор для рішення задач управління інформаційною безпекою в сучасних інформаційних системах полягає в урахуванні при формуванні оптимальної стратегії інформаційної безпеки результатів прогнозування на декілька циклів вперед, а також залежності способів дій сторін від інформації про протидіючу сторону. Таким чином, теорія ігор дозволяє запропонувати рекомендації по формуванню стратегії управління режимами роботи засобів інформаційної безпеки.

Впровадження теорії ігор у інформаційних системах пов'язано з роботами по теорії потенційної завадостійкості і по теорії статистичних рішень. Безпосередньо ж теорія ігор використовується лише для вивчення окремих ланок інформаційних систем і тільки в теорії інформації вона була використана для узагальнення теорії Шеннона.

Процес управління в ігрових системах завжди носить дискретний характер, так як кожна гра представляє собою послідовність окремих ходів. Процес, що управляється ігровою системою, може бути направлений або проти організовано діючого супротивника, або проти випадкового процесу. В першому випадку має місце „боротьба" двох або більшої кількості алгоритмів. В другому випадку має місце „боротьба" алгоритмів з випадковими збурюючими факторами.

В обох випадках можна чітко виділити сторони, що приймають участь у грі. Зазвичай в літературі розглядаються ігрові системи з двома діючими сторонами: А та Б. Сторона А – процеси або об'єкти, що управляються даною ігровою системою. Сторона Б – протидіюча система, дії якої підкоряються певному алгоритму, або ж випадкові збурюючі фактори.

Саме ігрові системи з двома учасниками мають найбільш важливе в сучасний період практичне застосування ігрових систем управління. Звичайно, можливі ігрові системи управління з трьома та більшою кількістю учасників подібно до того, як можливі ігри з трьома та більшою кількістю гравців [1].

Ігрові системи управління по своєму призначенню повинні зберігати працездатність та ефективність для широкого діапазону (множини) можливих дій Б сторони (в загальному випадку – всіх супротивних сторін). За цією ознакою ігрові системи управління відносяться до систем з мінімальною необхідною апріорною інформацією про Б сторону.

Повна апріорна інформація про Б сторону потрібна була б в тому випадку, якщо б ігрова система здатна була функціонувати тільки при суворо визначених діях Б сторони, що, очевидно, повністю знецінює застосування ігрової системи.

Основна задача будь-якої інформаційної системи полягає в передачі інформації з однієї точки простору в іншу. Інформаційна система являє собою мережу, що зв'язує два або більшу кількість пунктів (вузлів), оснащену технічними засобами передачі та прийому інформації і належним чином організовану систему інформаційної безпеки [2, 3]. Процес передачі сигналів зв'язку супроводжується дією перешкод супротивника, що в кінцевому рахунку приводить до втрати інформації і необхідності приймати рішення в умовах невизначеності. Невизначеність може виникати і з інших причин, оскільки прийняття рішень ґрунтується не на об'єктивних обставинах, а на суб'єктивних представленнях про них. У задачах зв'язку часто доводиться зустрічатися із ситуаціями, коли нема надійної основи для завдання статистики перешкод (або їхніх деяких характеристик), апріорних ймовірностей сигналів, значень функцій втрат, параметрів каналів зв'язку та т.ін., тому доводиться відмовлятися від використання усіх або частини таких характеристик. Відзначені обставини власне кажучи й визначають можливості використання ігрових методів для аналізу і синтезу інформаційних систем, постановки та рішення різноманітних

задач захисту інформації, що і складає зміст технічних додатків у інформаційних системах. Є також і особливі задачі, де конфлікти виступають у явному виді і мають антагоністичний характер. Сюди включаються питання протидії зловмисника і все те, що можна назвати "інформаційною війною" [4].

Особливістю інформаційного конфлікту підсистеми оперативного управління інформаційною безпекою і системи, яка їй протидіє є те, що протидіючі сторони, які мають декілька способів дій, можуть застосовувати їх багаторазово, вибираючи найкращий спосіб з урахуванням інформації про дії протилежної сторони. При цьому кожний крок вирішення конфлікту характеризується не фінальним станом, а деякою платіжною функцією. Традиційний ігровий підхід до аналізу завадозахищеності систем інформаційної безпеки не дозволяє врахувати багатокроковість конфлікту і не відображує залежність способів дій сторін від інформації про протилежну сторону, а відомий конфліктний підхід [5] на основі розрахунку фінальних ймовірностей перебування систем у стані виграшу до заданого моменту часу не відображує багатоваріантність дій сторін і неповну завершеність конфлікту на кожному кроці.

Тому виникає необхідність розробки методів оперативного (адаптивного) управління інформаційною безпекою залежно від наявності апріорної інформації про параметри протидіючої системи і реалізовані нею стратегії створення завад та несанкціонованого зйому інформації.

Для характеристики поточного стану конфлікту будемо використовувати показник завадозахищеності системи інформаційної безпеки (СІБ) $a_{ij} = P_{\text{пом}}$ при реалізації в ній *i*-ї, $i \in I = \{1, 2, \ldots n\}$, стратегії (способу) завадозахисту і застосуванні *j*-ї, $j \in J = \{1, 2, \ldots m\}$, стратегії (способу) створення завад, m і n - кількість стратегій завадозахисту і створення завад, реалізованих у СІБ і в системі, яка їй протидіє (ПС), відповідно.

Стороною А назвемо підсистему оперативного управління СІБ, стороною В – ПС, а величину a_{ij} – виграшем сторони А (програшем сторони В) у ситуації (i, j). При традиційному ігровому підході до аналізу завадозахищеності СІБ передбачається, що сторонам відома матриця гри і скінченна множина стратегій супротивника, але невідомо, яка стратегія реалізується в конкретній ситуації. У цьому випадку в матричній грі формалізується ситуація вибору стратегій завадозахисту в умовах невизначеності. Однак такий підхід не відображує динаміку конфлікту, а також можливість цілеспрямованого вибору стратегій завадозахисту на кожному кроці залежно від інформації про дії ПС. Тому пропонується для опису розглянутого конфлікту використати модель крокової матричної гри із запізнюванням і помилками в інформованості сторін про дії супротивника (матрично-ігрового процесу) [6]. Позначимо: $T_{\text{СІБ}}(T_{\text{ПС}})$ - час однократної реалізації стороною А (В) своєї чистої стратегії; $t_{\text{СІБ}}$ ($t_{\text{СП}}$) – час реакції сторони А (В), який дорівнює інтервалу часу від моменту початку реалізації стратегії стороною В (А) до моменту початку реалізації відповідної стратегії стороною А (В).

Будемо вважати, що сторонам відома: матриця гри $\mathbf{A} = (a_{ij})_m^n$, множини активних стратегій I, J і оцінки величин $T_{\text{СІБ}}(T_{\text{ПС}})$ і $t_{\text{СІБ}}$ ($t_{\text{СП}}$); матриця гри **A** є невиродженою і має рішення у вигляді ціни гри v і векторів оптимальних змішаних стратегій сторони А – $P^* = (P_1^*, P_2^*, \ldots, P_3^*, \ldots, P_n^*)$ і сторони В – $Q^* = (Q_1^*, Q_2^*, \ldots, Q_j^*, \ldots, Q_m^*)$; протягом часу гри T відсутня післядія, а множини I і J є незмінними.

Методика призначена для адаптивної зміни параметрів і режимів роботи СІБ за ігровим алгоритмом в залежності від наявності апріорної інформації про параметри ПС і стратегії створення нею завад засобам інформаційної безпеки.

Сутність ігрового алгоритму управління полягає в порівнянні великої кількості можливих даних в умовах якісно різних рішень, визначенні оптимального або найкращого з урахуванням всіх обмежень рішення та формування відповідної команди.

Постановка завдання.

Задано: матриця гри $\mathbf{A} = (a_{ij})_m^n$, множини чистих стратегій сторін А і В, для яких існує рішення в змішаних стратегіях (P^*, Q^*, v), а також ймовірнісно-часові характеристики протидіючої системи.

Стратегіями СІБ є параметри і режими роботи засобів засобів захисту інформації, стратегіями протидіючої системи – різні види навмисних завад та способи несанкціонованого зйому інформації.

Необхідно: визначити оптимальну змішану стратегію СІБ і необхідні ймовірнісно-часові параметри сторони А, що гарантують максимальний або заданий рівень її середнього виграшу за час $T >> T_{\text{СІБ}}$.

Обмеження:

– СІБ і протидіюча система мають в своєму розпорядженні скінчену кількість стратегій;

– свої стратегії сторони (А і В) використовують незалежно один від одного, тобто кожна зі сторін не має на початку гри інформації про дію, що здійснюється іншою стороною;

– системі інформаційної безпеки відомий час $\Delta t_{\text{оц}}$, за який протидіюча система зможе оцінити обстановку, прийняти рішення і змінити свої робочі параметри.

Задача параметричної оптимізації алгоритмів функціонування СІБ полягає у визначенні такої оптимальної стратегії $\grave{a}^* \in \grave{A}^*$, при якій забезпечується максимальна ефективність функціонування системи інформаційної безпеки протягом необхідного часу функціонування.

Для підвищення ефективності при вирішенні динамічних ігор використовується метод прогнозування.

Одним з можливих рішень ігор у змішаних стратегіях є збільшення швидкості реакції (зниження часу адаптації) однієї зі сторін, що дозволяє підвищити результативність використання стратегій.

З врахуванням трьох етапів циклу управління (контроль, ідентифікація й регулювання) визначимо критерії оптимізації $k_{\text{а}}$ СІБ, що бере участь у формуванні елементів ігрової матриці, на кожному етапі. Скороченню часу контролю буде сприяти зменшення кількості елементів вектора інформаційних параметрів h, що використовуються в трьохетапній ідентифікації та не впливають на якість контролю, а також зниження частоти сканування параметрів, які змінюються повільно

$$n(h_n) \to \min, \quad m(h_m^I) \to \min.$$

Час ідентифікації, що включає розрахунок елементів і рішення матричної гри, можна скоротити за рахунок реалізації принципу прогнозування і визначення обмеженої кількості найбільш імовірних стратегій протидіючої системи, завдяки чому розмірність ігрової матриці зменшується. Відповідно зменшується і кількість елементарних обчислювальних операцій: від $\left|S_{ij}\right|_{I \times J}$ до скороченого $\left|S_{ij}\right|_{I \times K}$, при K = 1, 2, 3.

Крім того, частина часу ідентифікації може поєднуватися з контролем і регулюванням параметрів. У цьому випадку етап регулювання для заздалегідь спрогнозованої стратегії ПС може починатися при наявності перших даних контролю про зміну стратегії протидіючою системою.

Коефіцієнт адаптації СІБ залежить від співвідношення $T_{\text{СІБ}} / T_{\text{ПС}}$ а значення $T_{\text{№2А}}$, $T_{\text{І Ѕ}}$ - від тривалостей часу регулювання і зміни режимів роботи засобів засобів захисту інформації, які залежать від їх стану в попередньому циклі. Тривалість переходу СЗІ зі стану H_n у стан H_m на етапах регулювання (H_n і H_m вектори станів засобів інформаційної безпеки) задається заздалегідь відомою квадратною матрицею часу переходу з будь-якого можливого (узятого з області визначення) стану в будь-який можливий: $\left|R_{(\text{ðåã})nm}\right| N \times M,\ n = \overline{1, N},\ m = \overline{1, M}.$ Елементами матриці будуть $T_{\text{ÑÇ}^{\text{ð}}nm}^{\text{ðåã}}$, що входять до складу $T_{\text{ÑÇ}^{\text{ð}}}^{\acute{I}}$ на етапі регулювання параметрів і зміни режимів роботи системи. Тоді процес переходу з H_n в H_m з врахуванням можливих проміжних станів може бути описаний апаратом однорідних марківських ланцюгів з дискретними станами в дискретному часі. Порядок переходу від $H_n(t)$ до $H_m(t+1)$ задається відповідною стратегією $a_i \in S_{\text{ÑÇ}^{\text{ð}}}$. Аналогічний стан протидіючої системи при переході визначається, як $\acute{I}_{\text{ Ï Ñ}n}(t)$ і $\acute{I}_{\text{ Ï Ñ}m}(t+1)$.

Тому задача умовної оптимізації часу адаптації на етапі регулювання полягає у виборі такої стратегії a^* на циклі $(t+1)$, при якій:

$$\begin{cases} T_{\text{ÑÇ}^{\text{ð}}}((t+1), \grave{a}^*) = \min\limits_{\grave{a}_i \in S_{\text{ÑÇ}^{\text{ð}}}} T_{\text{ÑÇ}^{\text{ð}}}(\acute{I}_{\ n}(t), \acute{I}_{\ m}(t+1), \grave{a}_i); \\ T_{\text{Ï Ñ}}((t+2), \grave{a}^*) = \max\limits_{\grave{a}_i \in S_{\text{ÑÇ}^{\text{ð}}}} T_{\text{Ï Ñ}}(\acute{I}_{\text{ Ï Ñ}n}(t+1), \acute{I}_{\text{ Ï Ñ}m}(t+2), \grave{a}_i) \end{cases} \quad (1)$$

за умови $T_{\text{ÑÇ}^{\text{ð}}} < T_{\text{Ï Ñ}}$, що й відбувається в процесі рішення гри за рахунок введення $k_{\text{а}}$ при розрахунку елементів матриці.

Чисельно точність передбачуваного значення функції виграшу задається деяким коефіцієнтом помилки прогнозування

$$k_{\text{ï ð}}(t+1|t) = \frac{\hat{\text{O}}(t+1)}{\hat{\text{O}}_{RL}(t+1)},$$

де $\hat{\text{O}}_{RL}(t+1)$ обчислена при досягненні (t + 1) у результаті моніторингу. Так, у випадку незмінної протягом ряду циклів стратегії ПС при Ф(t), відбувається корекція Ф(t + 1) за рахунок $k_{\text{ï ð}}(t+1|t)$, що входить до складу коефіцієнту $\beta_m(t+1)$, Це усуває систематичну помилку в розрахунках значень Ф(t) і деякою мірою впливає на вибір $a^*(t+1)$ у ході рішення матричної гри.

Оскільки коефіцієнт помилки прогнозування перебуває у зворотній залежності від коефіцієнта інформованості $k_{\text{inf}}^{à}$, функція $f(k_{\text{inf}}^{à}) = \left|k_{\text{ï ð}}(t+1|t) - 1\right|$. У цьому випадку має місце постановка наступної задачі умовної оптимізації:

$$k_{\text{inf}}^{à} \to \max,$$

де $\max k_{\text{inf}}^{à} = k_{\text{inf}}^{S}$ при обмеженні:

$$\left|k_{\text{ï ð}}(t+1|t) - 1\right| \le d_{\text{ï îì}},$$

де $\delta_{\text{пом}}$ – деяка центрована випадкова величина з нульовим математичним очікуванням і дисперсією δ^2, яка визначає деяке граничне значення помилки.

Розповсюджений спосіб рішення матричної гри в змішаних стратегіях, наприклад, методами лінійного програмування, істотно ускладнюється для матриць великої розмірності. Застосування декомпозиційних методів не завжди можливо, а ітеративні методи рішення, такі, наприклад, як метод Брауна-Робінсона, мають найчастіше недостатньо високу швидкість збіжності [1]. Як альтернативний може бути використаний метод динамічного програмування, що використовує результати короткочасного та довгострокового прогнозування.

Розглянемо алгоритм рішення матричних ігор, що використовує метод динамічного програмування. Стосовно до розглянутих випадків довгострокове прогнозування дозволяє з досить великим ступенем надійності обмежити кількість ймовірних стратегій протидіючої системи у наступних циклах управління до 2...4 і редукувати ігрову матрицю. Рішенням матричної гри з урахуванням принципу прогнозування на основі марківського підходу є оптимізація умовної стратегії систем інформаційної безпеки на N циклів вперед по прогнозованій стратегії протидіючої системи. Очевидно, що з ростом N, точність прогнозування знижується. У зв'язку із цим розглянемо випадок, коли N = 1. Можна виділити три етапи алгоритму формування оптимальної стратегії СІБ.

На першому етапі на підставі інформації про поточний стан засобів інформаційної безпеки, передбачуваного значення перехідних ймовірностей систем захисту інформації, застосованої на циклі управління t стратегії ПС $b(t)$, а також з врахуванням попередніх стратегій протидіючої системи формується оптимальна умовна стратегія $à^*(t+1|)t$:

$$à^*(t+1|)t = \arg\left[\max_{à \in S_{\text{ÑÇ}}} P(à(t), b(t), Í\ (t))\right]. \quad (2)$$

На другому етапі вирішується завдання прогнозування стратегії, яка використовується на циклі управління t +1 протидіючою системою і яка забезпечить мінімізацію функціонала

$$b^*(t+1|)t = \arg\left[\min_{b \in S_{\text{Ï Ñ}}} P(à^*(t+1), b(t+1))\right]. \quad (3)$$

На третьому етапі формується оптимальна стратегія управління СЗІ з урахуванням прогнозованої стратегії ПС і поточного стану засобів інформаційної безпеки:

$$à^*(t+1|t) = \arg\left[\max_{à \in S_{\text{ÑÇ}}} P(à(t+1), b^*(t+1|t), Í\ (t+1), b_m(t+1), k_{\text{â}}(Í\ (t+1)|Í\ (t)))\right]. \quad (4)$$

Для підвищення надійності результату алгоритм (2-4) може повторюватися обмежену кількість разів при наявності певної дисперсії розподілу ймовірностей застосування стратегії $à_1^*(t+1|t)\ ...à_n^*(t+1|t)$ з їх наступною оцінкою на основі критеріїв переваги, що вводяться. У випадку неможливості визначення такої стратегії $à^*(t+1)$, при якій втрати не перевищують

припустимого значення, вирішується завдання розширення множини допустимих стратегій СЗІ, після чого знову визначається $a^*(t+1)$. Аналогічно формуються стратегії СЗІ шляхом оптимізації умовної стратегії управління системи по прогнозованій на N кроків стратегії протидіючої системи. Третій етап алгоритму в цьому випадку буде мати вигляд:

$$\grave{a}^{*(N)}(t+N) = \arg[\max_{\grave{a}\in S_{\hat{N}\hat{C}^3}} P(\grave{a}(t+N), b^*(t+N \mid t+N-1),\ \acute{I}\ (t+N),\ \beta_m(t+N),$$

$$k_{\grave{a}}(\acute{I}\ (t+N) \mid \acute{I}\ (t+N-1))],\ N=2,\ 3...$$

Апарат марківських кіл використовується на другому і третьому етапах, що дозволяє розраховувати ймовірності застосування тієї або іншої стратегії на черговому циклі управління і вибору оптимальної стратегії.

Припустимо, що в циклі управління t використовується стратегія протидіючої системи: b_2. Нехай, за критерієм $\max_{\grave{a}_1} P_{i,2}(t) = P_{3,2}$ вибирається стратегія a_3 (табл. 1). Одночасно із цим реалізується алгоритм прогнозування. У табл. 1 представлений спрощений приклад прогнозованого переходу системи зі стану в циклі t у стан $(t+1)$ на основі неоднорідних марківських кіл [7]. Відповідно до принципу оптимальності [8], при пошуку оптимального рішення в багатокроковому завданні оптимізації вибір стратегії управління $a(t)$ на кожному кроці незалежно від початкового стану повинен бути спрямований на оптимізацію не тільки даного, але і всіх наступних кроків. З урахуванням прогнозування на $(t+N)$ кроків уперед (у цьому випадку, не більше трьох кроків) механізм вибору оптимальної стратегії $a^*(t)$ у циклі t буде також визначатися обчисленням зворотної функції Беллмана останніх прогнозованих $N-t+1$ циклів управління. Так, для $t=N$:

$$B_N(\acute{I}\ (N-1)) = \max_{\grave{a}(N)\in\Lambda_N^I(\acute{I}\ (N-1))} P_N(\acute{I}\ (N-1), \grave{a}(N)),$$

де $H(N-1)$ – стан СЗІ на $(N-1)$-му циклі управління; $a(N)$ стратегія управління на циклі N; $\Lambda_N(\acute{I}\ (N-1))$ – скінченна множина допустимих стратегій на циклі $(N-1)$.

Таблиця 1

Алгоритм прогнозованого переходу станів СЗІ

t	Процес прогнозування					$t+1$
1-й етап	2-й етап			3-й етап		
Рішення на циклі	Імовірність переходу $P_{3j}=1-k_N\Phi_{3j}$	$\min_{b_j}(1-P_{3j}(t+1))$		Імовірність переходу $P_{i4}=k_N\Phi_{i4}$	$\max_{a_1} P_{i2}(t+1)$	
a_3	P_{31} ⇒	b_1	b_4	P_{14} ⇒	a_1	a_{12}
	P_{32} ⇒	b_2		P_{24} ⇒	a_2	
	P_{33} ⇒	b_3		P_{34} ⇒	a_3	
	P_{34} ⇒	b_4		P_{44} ⇒	a_4	
	…	…		…	…	
	P_{3j} ⇒	a_j		P_{i4} ⇒	a_{i4}	
a_3; b_2						a_2; b_4

Метод Беллмана використовується для підвищення точності прогнозу, обґрунтованості вибору поточних стратегій і підтримки прийняття рішень пристроєм управління інформаційної безпеки.

Таким чином, у процесі умовної оптимізації з врахуванням поточної ігрової матриці будуть формуватися умовно оптимальні стратегії, що визначають фазову траєкторію СЗІ, починаючи із заключного циклу прогнозування $t=N$ до поточного значення t.

У цьому випадку в кожному циклі управління потрібне рішення оптимізаційної задачі, яка має наступний вигляд:

$$\begin{cases} k_{\text{inf}}^{\grave{a}} \to extr = k_{\text{inf}}^{s} \quad \text{ï ðè óì î â³ } n(h_n) \le n_{\ddot{a}\hat{i}\,\ddot{i}}, \\ m(h_m^I) \le m_{\ddot{a}\hat{i}\,\ddot{i}} \\ \dfrac{T_{\tilde{N}\tilde{C}^2}}{T_{\ddot{I}\,\tilde{N}}} \to \min \quad \text{ï ðè óì î â³ } T_{\tilde{N}\tilde{C}^2} < T_{\ddot{I}\,\tilde{N}} \dfrac{k_{\grave{a}}(t)}{a}; \\ k_{\grave{a}(\min)} \le k_{\grave{a}}(t) \le k_{\grave{a}(\max)}. \end{cases} \tag{5}$$

Основним обмеженням у виразі (5) є $k_{\grave{a}(\min)} \le k_{\grave{a}}(t) \le k_{\grave{a}(\max)}$. Коефіцієнт адаптації обмежений знизу мінімальною тривалістю перехідних процесів регулювання і обчислювальною потужністю центрального процесору, зверху – мінімальною тривалістю циклу управління протидіючої системи.

В залежності від результатів прогнозування формуються команди управління адаптації для зміни параметрів і режимів роботи засобів інформаційної безпеки. *З*апропонована методика дозволяє враховувати при формуванні оптимальної стратегії систем інформаційної безпеки результати прогнозування на N циклів вперед, а також залежності способів дій сторін від інформації про протилежну сторону. Для зменшення розмірності ігрової матриці обмежується кількість найбільш небезпечних стратегій протидіючої системи, а частина часу ідентифікації поєднується з контролем і регулюванням параметрів.

Таким чином, теорія ігор дозволяє запропонувати рекомендації по формуванню стратегії управління режимами. Причому, принаймні, для певних типів конфліктів і матриць виграшів ці рекомендації дозволяють системі інформаційної безпеки отримати виграш і досягнути поліпшення своїх технічних характеристик.

Література

1. Оуэн Г. Теория игр / Г. Оуэн. – М.: Мир, 1971. – 230 с.
2. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия. – Телеком, 2000. – 452 с.
3. Ярочкин В.И. Безопасность информационных систем. – М.: Ось, 1996. – 320 с.
4. Коржик В.И., Кушнир Д.В. Теоретические основы информационной безопасности телекоммуникационных систем. — С.-Пб.: СПбГУТ, 2000. — 134 с.
5. Дружинин В. В. Введение в теорию конфликта / В. В. Дружинин, Д. С. Конторов, М. Д. Конторов. – М.: Радио и связь, 1989. – 288 с.
6. Радзиевский В. С. Информационное обеспечение радиоэлектронных систем в условиях конфликта / В. С. Радзиевский, А. А. Сирота. – М: ИПРЖР, 2001. – 574 с.
7. Дынкин Е. Б. Управляемые марковские процессы и их приложения / Е. Б. Дынкин, А. А. Юшкевич. – М.: Наука, 1975. – 248 с.
8. Стеклов В. К. Оптимізація та моделювання пристроїв і систем зв'язку: Підр. для вищ. навч. закл / В. К. Стеклов, Л. Н. Беркман, Є. В. Кільчицький; під ред. В. К. Стеклова. – К.: Техніка, 2004. – 576 с.