15.**Fredericks J. C., Saunders N. R., Broadfoot J. T.** Recent developments in positive displacement shotcrete equipment. Shotcreting, Publication Sp—14 ACI.

16..**Ir O. K-,** Maltiple laxer shotcrete tunnel lining. Shotcreting, Publication Sp-14 ACI.

17.**Reading T. J.** Shotcrete as a construction material. Stfpiereiihg, Publication SP-14, ACI.

18.**Kovernichenko L,** Shishkin A. Regulation of the influence of the structure of inorganic binders on their properaties//Technology audit and production reserves.2018.№3/1(41).

19.**Кузнецова А.М.** Технология вяжущих веществ и изделий из них.// Учебник для студентов ВУЗов М. Высш. шк., 1963.-455 с.

20.**Мощанский Н.А.** Повышение стойкости строительных материалов и конструкций, работающих в условиях агрессивных сред.// М. Госстройархиздат, 1962. - 235 с.

21.**Нікіфоров О.П**. Важкі бетони на шлаковміщуючих в'яжучих з комплексними модифікаторами.// Дн-ськ Пороги, 1996. - 232 с.

22.**Пшінько О.М.** Підводне бетонування та ремонт штучних споруд: //Монографія. – Дніпропетровськ: Пороги, 2000. – 411 с.

23.**Чернявський В.Л.** Адаптація бетону. //Дн-ськ Нова Ідеологія, 2002. - 116 с.

24.**Brux G. Neure** Betonherstellungs und Verarbeitungs verfahren, Der Eisen bauingenieur, 1956 № 3.

25. Chefdeville J. Beton de blocage et mortar actives, «Annales de b'institut technique du batiment et travaux publics.», 1959 № 144.

26.**Clark B. E.** Teoretical basis of pressure grout penetration, Journal of Amer. Concr. Inst., 1955, vol. 27 № 2.

27.**Fredericks J. C., Saunders N. R., Broadfoot J. T**. Recent developments in positive displacement shotcrete equipment. Shotcreting, Publication Sp—14 ACI.

28.**Ir O. K-**, Maltiple laxer shotcrete tunnel lining. Shotcreting, Publication Sp-14 ACI.

29.**Reading T. J.** Shotcrete as a construction material. Stfpiereiihg, Publication SP-14, ACI.

30.**Steenson H. N.** Fast set shotcrete in concrete construction. «ACI Journal», ProcV-71, 1974 № 6, pp. 289—295. Zlnda S. G. Properties of sand—mix shotcrete. Shotcretmg, Publicaion Sp-14 ACI.

31.**Агурин Д. П., Воробьев И. П., Нестеров В, Г**. Торкретирование тепловых агрегатов. М., Стройиздат, 1972.

32.**Захарченко Г. А., Хаютин Ю, Г., Совадов И.П** Раздельное бетонирование конструкций с нагнетанием активированного раствора в крупный заполнитель. М., ЦБТИ ЦНИИОМТП, 1968.

33.**Избаш С, В., Слиеский П. М**. Гидравлические основы возведения плотин замывом каменной наброски песком. // Труды МЭИ, вып. XXXXVI.M., 1961.

34.**Картелев И. Е.** Инъекционный способ бетонирования гидротехнических и других массивных сооружений. //Автореф. дис. на соиск. уч. степени. Л., 1954.

35.**Лермит Р.С** Проблемы технологии бетона. М., Госетройиздат, 1959.

36.Рекомендации по применению активированного торкрета в конструкциях сооружений. ВНИИГ. Л, Энергия, 1973.

37.**Третьяков А. К.** Исследование способа раздельного бетонирования гидротехнических сооружений. //Автореф. дис. на соиск. уч. степени. М., 1956.

38.**Brux G.** Neure Betonherstellungs und Verarbeitungs verfahren, Der Eisen bauingenieur, 1956, № 3.

39.**Chefdeville J.** Beton de blocage et mortar actives, «Annales de b'institut technique du batiment et travaux publics.», 1959, № 144.

40.**Касаткин А.Г.** Основные процессы и аппараты химической технологии. М, «Химия»1971.

41.**Рыбьев И.А.** Строительные материалы на основе вяжущих веществ. –М: Высш.школа, 1978.-309 с.

42.**П.В.Кривенко,К.К.Пушкарьова**Довговічність шлаколужного бетону. // К. Будівельник, 1993. - 224 с.

43. **Москвин В.М.,. Иванов Ф.М Алексеев С.Н. Гузеев Е.А.; под общ. ред. Мсквина В.М..** Коррозия бетона и железобетона, методы их защиты // - М.: Стройиздат, 1980. - 536 с.

44.**Шестоперов С.В.** Долговечность бетона транспортных сооружений. // – М.: Изд-во «Трансорт», 1966. – 400с.

Рукопис подано до редакції 04.04.2019

УДК 004.056:007 (045)

Г.В. ДАНИЛІНА*, Л.Л. ЖУКОВА, кандидати техн.наук, доценти,
Н.В. АНДРУСЕВИЧ, зав. відділення
Криворізький коледж національного авіаційного університету
С.Л. ЦВІРКУН, канд.техн.наук, викл., Криворізький національний університет

СТОХАСТИЧНЕ КЕРУВАННЯ ПАРАМЕТРАМИ УРАЗЛИВОСТЕЙ З ВИКОРИСТАННЯМ ЕСКАЛАЦІЙНИХ ПАСТОК

Мета: розробити математичну модель і методику захисту комп'ютерної мережі від зовнішніх і внутрішніх загроз в умовах апріорної невизначеності стану мережі і ризику виникнення конфлікту з активним (розумним) партнером. Провести систематизацію на основі математичного апарату статистичної теорії ризику, теорії конфлікту, теорії масового обслуговування, дослідження операцій. Статистично оцінити потенційну ефективність і асимптотичні характеристики систем захисту.

Методи: спостереження, експеримент.

Наукова новизна: доведено, що при використанні методів конфліктного управління процесами захисту комп'ютерних мереж можна добиватися виграшу, навіть якщо противник має помітну перевагу в ресурсах. Проведено систематизацію на основі математичного апарату статистичної теорії ризику, теорії конфлікту, теорії масового обслуговування, дослідження операцій.

Практична значимість: розроблено математичну модель і методику захисту комп'ютерної мережі від зовнішніх і внутрішніх загроз в умовах апріорної невизначеності стану мережі і ризику виникнення конфлікту з активним (розумним) партнером. Рішення даної задачі досягнуто шляхом рефлексивного управління – урахування сильних і слабких сторін противника, цілеспрямованого виснаження його ресурсів в атаках на хибні об'єкти і псевдосервіси. На основі теорії керованих марковських процесів запропонований метод конфліктного управління з прогнозуванням розвитку ситуації, покрокової ідентифікації параметрів і стану і корекції за наслідками поточного аналізу.

Результати: розроблена в рамках загальної теорії конфлікту стратегія відволікання ресурсів противника на псевдосервіси може дати виграш навіть в разі переваги ресурсів атаки над ресурсами захисту. Розроблено математичну модель і методику захисту комп'ютерної мережі від зовнішніх і внутрішніх загроз в умовах апріорної невизначеності стану мережі і ризику виникнення конфлікту з активним (розумним) партнером. Проведено систематизацію на основі математичного апарату статистичної теорії ризику, теорії конфлікту, теорії масового обслуговування, дослідження операцій. Статистично оцінено потенційну ефективність і асимптотичні характеристики систем захисту.

Ключові слова: математична модель, ескалаційна пастка, метод конфліктного управління, комп’ютерна мережа, псевдосервіс.

doi: 10.31721/2306-5451-2019-1-48-114-121

Проблема та її зв'язок з науковими та практичними завданнями. В даний час спостерігається великий інтерес до методів аналізу та оптимізації систем захисту комп'ютерних та об'єднаних мереж від атак і несанкціонованих вторгнень. Наводиться велике число прикладів таких систем, розробок різних протоколів, технологій, проектів і пов'язаних з ними міркувань, висновків та прогнозів. На жаль, систематизація в цій області знань на основі математичного апарату статистичної теорії ризику, теорії конфлікту, теорії масового обслуговування, дослідження операцій тощо займає в задачах побудови систем захисту вельми скромне місце. Прогалинами в цьому відношенні страждають роботи навіть провідних фахівців у цій галузі. Крім того, відсутні роботи по статистичному оцінюванню потенційної ефективності і асимптотичним характеристикам систем захисту. У даній роботі зроблена спроба якщо не повністю закрити цю нішу, то хоча б намітити шляхи постановки та розв'язання згаданих проблем.

Аналіз досліджень і публікацій. Судячи з результатів аналізу численних статей, монографій, матеріалів наукових і практичних конференцій, завдання захисту інформаційних ресурсів комп'ютерних мереж від атак з боку зовнішніх і внутрішніх порушників ніколи не втратить свою актуальність. У цей час опубліковані переліки декількох тисяч загроз та уразливостей інформаційно-комунікаційних систем. Зокрема, найбільш детальним описом такого роду є відкритий стандарт Європейського Союзу IT Baseline Protection Manual [1] обсягом більше чотирьох тисяч сторінок. Однак організація безпеки даних - не тільки систематизація, виявлення і відображення загроз, головне - управління ризиками, своєчасні превентивні заходи для зниження ризику загроз, щоденна робота по системному забезпеченню безпеки [2]. Для вирішення даного завдання вже недостатньо виявляти і реагувати на дії порушників. Необхідно не тільки прогнозувати такі дії, виключати уразливості в системах мережного захисту, але і відволікати зловмисників від мережних вузлів, в яких здійснюється зберігання і обробка інформаційних ресурсів.

Більш як десятиліття тому виникло розуміння, що пряме протиборство з шкідливими мережними впливами є практично марним. Був зроблений цілком логічний висновок про необхідність застосування методів, узятих з арсеналу системного аналізу, дослідження операцій у військовій справі і, нарешті, радіоелектронної боротьби - радіоелектронної і радіорозвідки, радіоелектронної протидії, дезінформації та ін.

Найбільший інтерес привернув метод так званої "медової пастки" [3] - заманювання на помилкові інформаційні об'єкти, що володіють високою вразливістю. В роботі [4] такі медові пастки названі псевдосервісами. Цілі колективи працювали над різноманітними проектами медових пасток [5,6]. Однак в результаті пошуку і аналізу численних літературних джерел нами були виявлені лише дві статті, що заслуговують на увагу [7,8]. Зокрема, в роботі [8] глибоко і всебічно опрацьований теоретичний підхід до оцінювання ефективності медових пасток (за термінологією статті - хибних інформаційних систем).

Однак в доступних нам джерелах не розглянуті питання аналізу можливої реакції супротивника у разі виявлення ним медових пасток. Також не розглянуті методи виключення або хоча б мінімізації подій виявлення.

Постановка задачі. З урахуванням вищевикладеного в даній роботі поставлено мету - розробити метод управління процесом захисту інформаційної системи на основі теорії конфлікту [9] і керованих марківських процесів [10].

Конфлікт не може розглядатися як задача оптимізації. При рівних ресурсах сторін "оптимальність" означає припинення конфлікту, а при нерівних - поразку більш слабкої сторони з імовірністю одиниця. Теоретично в конфлікті можливий виграш меншими силами. Проте, для досягнення виграшу з ймовірністю вище, ніж величина другого порядку малості, необхідно мати у своєму розпорядженні ресурси одного порядку з ресурсами атакуючої сторони.

Конфлікт з розумним противником не може бути розв'язаний і в рамках теорії адаптації. Своїми активними діями супротивник з імовірністю, що прямує до одиниці, досягне максимального виграшу. Ми ж, адаптуючись до умов, які постійно погіршуються, врешті-решт опинимося в найбільш невигідній ситуації.

Тому основними завданнями, які необхідно вирішити для досягнення поставленої мети, є:

аналіз можливих стратегій конфлікту і вибір найбільш перспективних стратегій для даної задачі;

вибір математичного апарату для опису процесів розвитку конфлікту;

розробка математичної моделі конфлікту;

отримання асимптотичних характеристик ефективності.

Викладення матеріалу та результати. Відповідно до загальної теорії конфлікту процеси протиборства між атакуючої і захищається сторонами описуються диференційно-різницевими рівняннями або рівняннями з аргументами, що відхиляються [11]. Це припущення справедливо для дискретних систем з запізненням, якими є комп'ютерні мережі й розподілені інформаційні системи.

У загальному випадку

$$\begin{cases} z`_{ids}(t) = f_1(t, z_{ids}(t), ....., z_{ids}(t-\tau_1), u_1(t), v_2(t-\tau_2), \zeta(t)); \\ z`_{icm}(t) = f_2(t, z_{icm}(t), ..., z_{icm}(t-\tau_2), u_2(t-\tau_2), v_1(t); \eta(t)), \end{cases} \quad (1)$$

де z_{ids} і z_{icm} – вектори стану систем S_{ids} і S_{icm} відповідно; $u_1(t)$ и $u_2(t)$ – вектори управлінь в S_{ids} і S_{icm} відповідно; $v_1(t)$ – вектор дій S_{ids} на S_{icm}; $v_2(t)$ – вектор дій S_{icm} на S_{ids}; $\xi(t)$ і $\eta(t)$ – вектори випадкових збурень, які діють на S_{ids} і S_{icm} відповідно; τ_1 и τ_2 – запізнення у векторах S_{ids} і S_{icm} відповідно.

Ефективність E_1 системи S_{ids} й ефективність E_2 системи S_{icm} на інтервалі спостереження T у загальному випадку являють собою нелінійні функціонали станів z_{ids}, z_{icm} и векторів $\xi(t)$, $\eta(t)$ відповідно. З рівняння (1) випливає їх взаємна залежність.

Якщо врахувати фактор нормалізації випадкових процесів у великих системах [12], то можна застосувати для вирішення рівнянь (1) метод гаусовської апроксимації в малій околиці точок екстремуму E_1 і E_2. У цьому разі вирази для ефективностей мають вигляд

$$E_1 = \int_0^T z_{ids}(t)dt, E_1 \to \max_{v_1} E_2 = \int_0^T z_{icm}(t)dt; E_2 \to \max_{v_2}. \quad (2)$$

Мета кожної системи - максимально підвищити свою ефективність за рахунок зниження ефективності супротивної сторони. Однак результат докладених зусиль стане відомий тільки в момент часу T. На інтервалі спостереження $0 \le t \le T$ можна виробляти найкращі управління $u_1(t)$, дії $v_1(t)$ та прогнозувати кінцевий результат, тільки спираючись на припущення про стратегії поведінки супротивника й дані про поточні стани z_{ids} и z_{icm}. Включення в рівняння (1) функцій $v_1(t)$ означає відволікання частини ресурсу на формування захисних або контратакують впливів. Отже, необхідно вирішувати задачу конфлікту або з додатковим критерієм мінімізації частки ресурсу, що відводиться на захист, або з обмеженням на допустимий витрата цієї частки ресурсу. Схема моделі конфлікту [1] між сторонами атаки S_{icm} та захисту S_{ids}, модифікована для випадку застосування стратегій ескалації в псевдосервіси (пастки, хибні інформаційні системи), наведена у роботі [4]. Модель реального конфлікту, як правило, є нелінійною, але для отриман-

ня асимптотичних оцінок при досить великому інтервалі спостереження (і, відповідно, при великому числі кроків розвитку конфлікту) є припустимим робити покрокову лінеаризацію моделі з екстраполяцією на основі методів кореляції та регресії [13]. Для пошуку коефіцієнтів екстраполяції лінеаризованої моделі розроблено модифіковану покрокову процедуру з заміною та примусовим включенням незалежних змінних. При цьому усунення з вибірки незалежних змінних X_1, X_2, …, X_p (активні ресурси та псевдосервіси) відсутнього значення X_i, $1 \le i \le p$ не є необхідним, оскільки воно може приводити до втрати про змінні X_1, X_2, … X_{i-1}, X_{i+1} … X_p інформації, яка доставляється елементом X_i. Теоретично можна залишити цей елемент у вибірці та використати виміри, що містяться в ньому, для обчислення вектора середніх значень $\vec{\mathbf{X}}$ та матриці коваріацій R_x.

У реальній ситуації для отримання цих даних приходиться використовувати наближені методи:

видалення елементів, лишаючи тільки комплектні елементи, тобто елементи з повністю присутніми значеннями;

підстановку середнього: замість відсутнього значення X_i підставляється середнє значення $\overline{x_i}$, завдяки чому результуюча вибірка комплектується до повного об'єму n;

попарного викреслювання, підстановки регресії тощо.

На жаль, для будь-якого зі згаданих методів їх статистичні властивості частіше за все невідомі, тому немає гарантій, що отримані оцінки будуть незміщеними. Тому елементи вибірки та/або змінні з відсутніми значеннями повинні бути видалені так, щоб забезпечити баланс між числом змінних і числом елементів, що залишилися. Іншими словами, максимізується число комплектних елементів вибірки: якщо елемент містить багато пропусків, його треба усунути. З іншого боку, якщо значення будь-якої змінної невідомо для більшості елементів, треба видалити цю змінну. Тоді можна застосовувати стандартні методи множинного регресійного аналізу [14].

На рис. 1 зображено математичну модель процесів розвитку конфлікту з передбаченням та виправленням помилкових припущень (модель типу "предиктор-коректор" [15]).

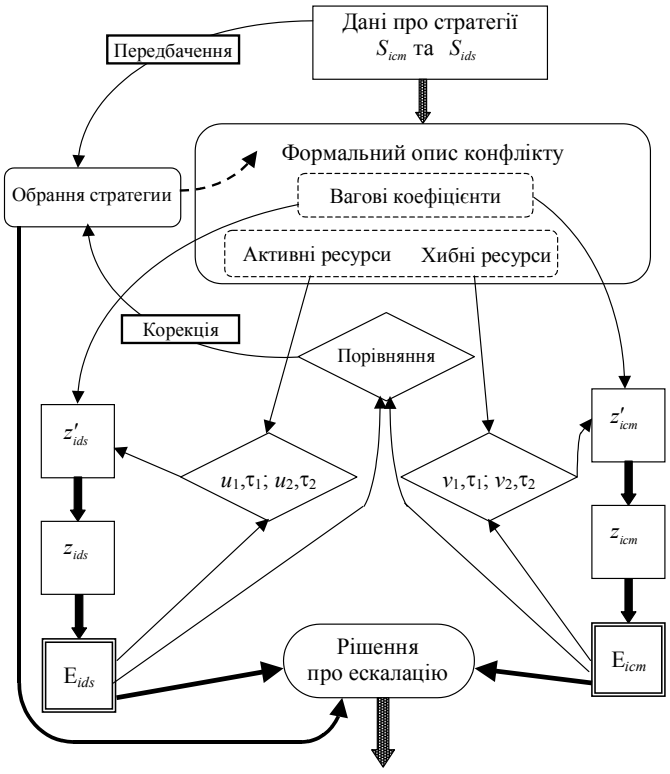

Рис. 1. Схема лінеаризованої моделі конфлікту з можливою ескалацією в псевдосервіси

Стратегії протидії і атак, розроблені відповідно до класичної теорії конфлікту [9] і модифіковані для конкретної розглянутої задачі, наведені в [4]. Тут же розглянемо набір найбільш наочних стратегій захисту:

ешелонування рубежів захисту типу "зовнішня - демілітаризована - внутрішня зони безпеки";

відмова від отримання - просте повернення підозрілого трафіку;

розподілена відмова від отримання - трансляція підозрілого трафіку на кілька точок і повернення трафіку з усіх цих точок;

насичення рубежів захисту псевдосервісамі з відтворенням добре відомих вразливостей - затягування противника в ескалаційну пастку.

В системі захисту, заснованої на теорії конфлікту, передбачаються активні дії по відбиттю атаки. Тут розглядаються теоретичні моделі і методи аналізу, прогнозу розвитку конфлікту і оптимізації послідовностей захисних дій. Щодо правових аспектів адекватності заходів контратаки передбачається лише, що оцінка цієї адекватності в технічних системах може бути зроблена досить точно і об'єктивно.

Динамічні характеристики процесу розвитку конфлікту з ескалацією в псевдосервіси.

Процес розвитку конфлікту є розгалуженим напівмарківським процесом, перехідні і фінальні ймовірності якого залежать від співвідношення стратегічних $S(S_{ids},S_{icm})$ й енергоінформаційних (E_{ids},E_{icm}) ресурсів сторін. Різновидом розгалуженого процесу є циклічний розгалужений процес, формально схожий з процесом загибелі та розмноження. Однак при всій зовнішній схожості цих процесів циклічними розгалуженими процесами є тільки процеси, що мають дві вершини (рис. 2).

Поточний стан процесу можна записати в вигляді деякого функціоналу, $\delta R = \Psi[\varphi(S_{ids},E_{ids}),\varphi(S_{icm},E_{icm})]$ яким характеризується інтегральний виграш від застосування тієї чи іншої стратегії S_{ids} з урахуванням інтенсивності її застосування $M_2[E_{ids}]$. Власне стратегія оцінюється по своїй інформаційній цінності, а інтенсивність - з енергетичного ресурсу (наприклад, за кількістю точок, з яких проводиться розподілена атака). В якості першого наближення для вибору виду функціоналу можна взяти адитивну міру множини стратегій, а відносний вплив конкретної стратегії врахувати ваговими коефіцієнтами або функціями.

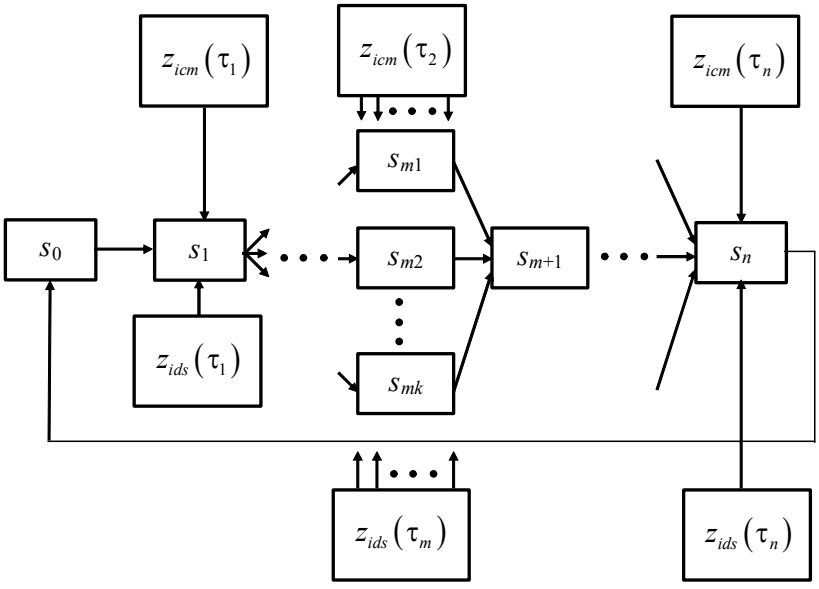

Рис. 2. Циклічний розгалужений процес конфлікту. Імовірності станів на *j* - му етапі

$$p_{ij}, \quad i=\overline{1,k}, j=\overline{1,n}, \quad \text{причому} \quad \sum_{i=1}^{k} p_{ij} = 1$$

Розглянемо алгоритмічну модель конфлікту між розподіленими системами атаки і захисту. Схема процесу моделювання атакуючих і контратакуючих потоків зображена на рис. 3.

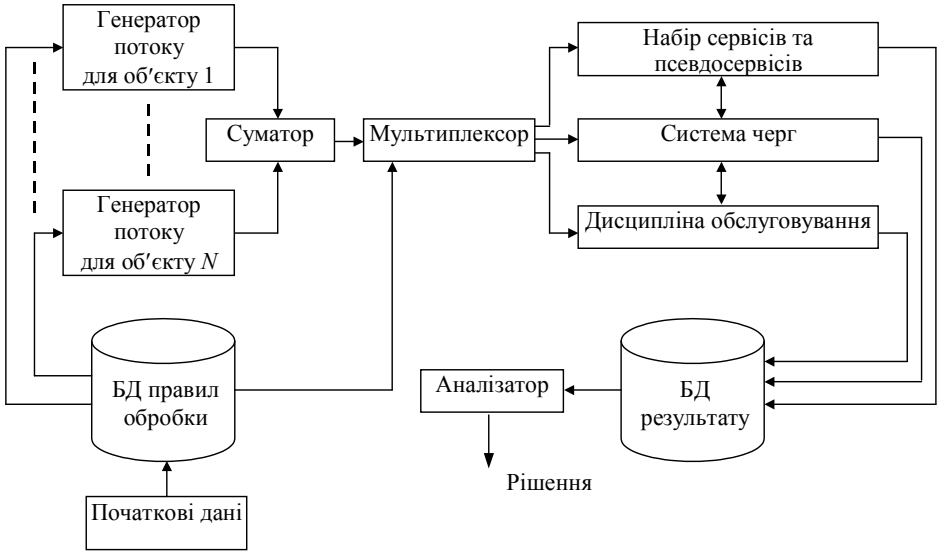

Рис. 3. Алгоритмічна модель

Як видно з рис. 3, рішення про вибір напрямку розвитку конфлікту приймаються на підставі результатів повного аналізу параметрів і стану системи, наявних вихідних даних і поточної інформації про характеристики мережного трафіку.

Мають місце послідовності дій і відповідних захисних заходів (пасивних, активних або й тих, і інших). Припустимо, що в результаті атаки ймовірність штатного функціонування об'єкта знижується, можливо, до нуля, а в результаті застосування відповідної захисного заходу ймовірність функціонування об'єкта підвищується, можливо, аж до вихідної величини. Таким чином, в кожен момент часу система може перебувати в одному з N можливих фазових станів ϕ_1, ϕ_2 ... ϕ_N, характеризують поточну ймовірність функціонування об'єкта. Відомі початковий стан системи (в початковий момент часу t_0 вона знаходиться в стані $\Psi_0 = \phi_i$) і однокрокові ймовірності переходу $\rho_{ik} = P\{\Psi_l = \phi_k | \Psi_{l-1} = \phi_i\}$, $i,k=\overline{1,N}$ Отже, якщо ігнорувати випадковий характер часу очікування і цікавитися тільки моментами переходу, то процес $\psi_l = \psi(t_l)$ є вкладений однорідний ланцюг Маркова [6]. Імовірність переходу ρ_{ik} повністю визначається i-м станом об'єкта і результатами k-ї атакуючої дії.

Затримки τ_1 і τ_2 в системах S_{ids} і S_{icm} являють собою дискретні процеси $z_{ids}(\tau_1), z_{icm}(\tau_2)$, які не обов'язково є марківськими. Однак це не критично для подальшого аналізу, оскільки самі величини $\rho_{mn}, m,n \in M$, дають вичерпну інформацію про еволюцію конфлікту.

Порівняємо кожному з ненульових елементів ρ_{ik} матриці ймовірностей переходу випадкову величину ζ_{ik} з функцією розподілу $F_{ik}(t) = F_{ik}(\tau_{ik} \le t)$. У розглянутій задачі випадкову величину ζ_{ik} будемо трактувати як час перебування атакується об'єкта в стані ϕ_i за умови, що наступним станом, в яке перейде об'єкт, буде ϕ_k. При цьому величина ζ_{ik} вважається не негативною і безперервною з щільністю ймовірності $w_{ik}(t)$. При такій інтерпретації величину ζ_{ik} можна назвати часом знаходження об'єкта в стані ϕ_i до переходу в стан ϕ_k.

Припустимо, що точка, яка відображає поведінку системи в просторі станів, залишиться в стані ϕ_i впродовж часу ζ_{ij}, до того, як вона перейде в ϕ_j (див. рис. 4, 5). По досягненні стану ϕ_j «миттєво» (відповідно до матриці ймовірностей переходу $\{\rho_{ik}\}$) обирається наступний стан $\phi_n, n = \overline{1,N}$. Тут «миттєвість» трактується в тому сенсі, що тривалість переходу є величиною другого порядку малості в порівнянні з мінімальною тривалістю перебування в поточному стані.

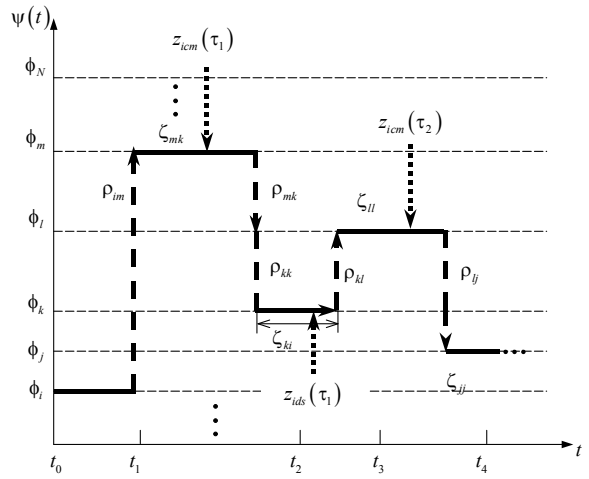

Рис. 4. Зміна ймовірностей функціонування об'єкта з системою захисту $z_{icm}(\tau_n) \succ z_{ids}(\tau_n)$

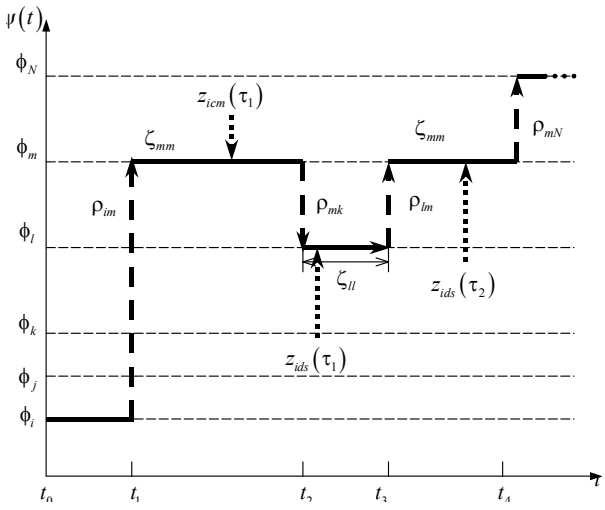

Рис. 5. Зміна ймовірностей функціонування об'єкта з системою захисту $z_{ids}(\tau_n) \succ z_{icm}(\tau_n)$

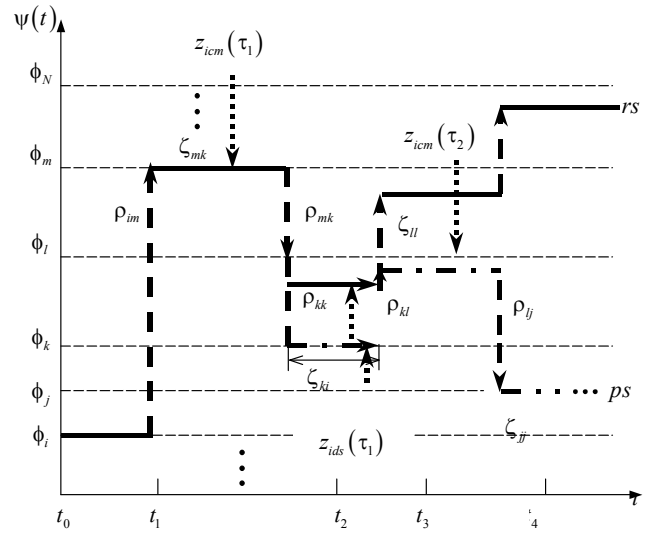

Рис. 6. Зміна ймовірностей функціонування об'єкта з системою захисту. *rs* – реальний сервіс; $z_{icm}(\tau_n) \succ z_{ids}(\tau_n)$; p_{ps}=1-ε, ε<<1 p_{ps} – ймовірність відволікання супротивника на псевдосервіс *ps*

Якщо для точки, що відображає поведінку системи і знаходиться в l-му стані, з імовірністю переходу ρ_{ll} знову обирається стан l, горизонтальна частина траєкторії руху точки позначається лінією зі стрілкою на кінці, як це зображено на графіках, див. рис. 4–6. Вираз $x \succ y$ означає домінування *x* над *y*.

Після того, як наступний стан ϕ_i обраний, час очікування в поточному стані ϕ_k вважається рівним ζ_{ik} з функцією розподілу $F_{ki}(t)$ або, відповідно, з щільністю імовірності $w_{ki}(t)$. Цей процес надалі необмежено триває. Кожен раз незалежно вибираються наступний стан і час очікування. Якщо через $\Psi(t)$ позначити стан системи, в якому вона знаходиться в момент часу *t*, то отриманий випадковий процес є напівмарківським. При заданому початковому стані подальшу поведінку процесу повністю визначається матрицею ймовірностей переходу $\{\rho_{ik}\}, i,k = \overline{1,N}$, и матрицею функцій розподілу $\{F_{ki}(t)\}$.

Висновки та напрямок подальших досліджень. На закінчення треба ще раз підкреслити, що силова протидія атакам і вторгненням в комп'ютерні мережі вимагає відволікання великих ресурсів і завершується успіхом лише в рідкісних випадках, наприклад, для випадку "розподілена атака - розподілений захист". У той же час розроблена в рамках загальної теорії конфлікту стратегія відволікання ресурсів противника на псевдосервіси може дати виграш навіть в разі переваги ресурсів атаки над ресурсами захисту.

Великий інтерес представляють розгалужені ескалаційні пастки з імітацією активної боротьби з супротивником шляхом стохастичного управління еволюцією вразливостей псевдосервісів (медових пасток). Ці задачі планується дослідити у подальшому.

Список літератури

1. http://www.iso27000.ru/standarty/bsi-it-baseline-protection-manual
2. Секреты и ложь. Безопасность данных в цифровом мире / **Б. Шнайер.** – СПб.: Питер, 2003. – 368 с

3. Spitzner L. Honeypots: tracking hackers. Addison-Wesley, 2002. – 480 pp.
4. **Виноградов Н. А.** Управление псевдосервисами в защищенных информационных системах на основе теории конфликта // Н. А. Виноградов, Г. В. Данилина, Д. В. Домарев, Я. В. Милокум – Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – №6(34). – с. 5 - 12.
5. https://www.projecthoneypot.org/
6. www.honeynet.org
7. **Котенко И. В., Степашкин М. В.** Обманные системы для защиты информационных ресурсов в компьютерных сетях // Труды СПИИРАН, Вып. 2, т. 1. – СПб.: СПИИРАН, 2004. с/ 211 - 230
8. **Язов Ю. К., Сердечный А. Л., Шаров И. А.** Методический подход к оцениванию эффективности ложных информационных систем // Вопросы кибербезопасности №1(2), 2014. – с. 55 – 60.
9. **Дружинин В.В., Конторов Д.С., Конторов М.Д.** Введение в теорию конфликта. – М.: Радио и связь, 1989. – 288 с.
10. **Дынкин Е.Б., Юшкевич А.А.** Управляемые марковские процессы и их приложения. – М.: Наука, 1975. – 338 с.
11. **Эльсгольц Л.Э., Норкин С.Б.** Введение в теорию дифференциальных уравнений с отклоняющимся аргументом. – М.: Наука, 1971. – 296 с.
12. **Казаков И.Е.** Статистическая динамика систем с переменной структурой. – М.: Наука, 1977. – 416 с.
13. **Афифи А., Эйзен С.** Статистический анализ: Подход с использованием ЭВМ. Пер. с англ. – М.: Мир, 1982. – 488 с.
14. **Draper N.R.** Applied regression analysis, 3rd Ed. / N.R. Draper, H. Smith. - John Wiley & Sons, 1998. - 736 p.
15. **Mosteller F.** Data Analysis and Regression: A Second Course in Statistics / F. Mosteller, J. W. Tukey. - Pearson, 1977. - 588 p.

Рукопис подано до редакції 10.04.2019

УДК 658.38:621.1

В.Г. НАЛИВАЙКО*, канд. техн. наук, доц., О.Г. МОВЧАН, канд. хим. наук, доц.,
К.В. ЛОСЬЕВ, ассист., Криворожский национальный университет

ВЛИЯНИЕ ПРОФИЛАКТИЧЕСКИХ РЕМОНТНЫХ РАБОТ НА УМЕНЬШЕНИЕ ЗАБОЛЕВАЕМОСТИ РАБОТНИКОВ ПРЕДПРИЯТИЙ ТЕПЛОСНАБЖЕНИЯ

Цель. Целью данной работы является разработка способов уменьшения заболеваемости работников предприятий теплоснабжения и водоснабжения и повышение безопасности труда при эксплуатации и ремонтах теплотрасс и теплогенерирующего оборудования. Также необходимо определить наиболее травмоопасные виды работ и специальности работников предприятий теплоснабжения их выполняющие, предложив способы уменьшения аварийной производственной нагрузки на них. Уменьшение аварийных работ может быть достигнуто путем проведения профилактических работ на теплотрассах и теплогенерирующем оборудовании, сокращая при этом количество опасных и вредных видов работ, а так же трудовые и материальные затраты, связанные с их выполнением.

Методы исследования. Исследования проводились с использованием математико-статистического метода экспертных оценок. Метод позволяет оперативно выявить наиболее проблемные и опасные работы предприятий теплоснабжения, возникающие как в процессе эксплуатации оборудования и теплотрасс, так и с внезапными аварийными ситуациями. Таким образом, можно определить перечень профилактических работ, которые должны быть выполнены в первую очередь.

Научная новизна. Исследования с использованием математико-статистического метода экспертных оценок позволят быстро определить первоочередность видов профилактических ремонтных работ на предприятиях теплоснабжения и предупредить аварийные ситуации.

Практическая значимость. Полученные выводы по результатам исследований позволят разработать рекомендации по уменьшению количества аварийных работ на теплотрассах. Определив наиболее травмоопасные виды работ и специальности работников предприятий теплоснабжения, которые их выполняют, необходимо уменьшить производственную загрузку, связанную с аварийными работами через проведение профилактических работ на наиболее потенциально опасных аварийных участках.

Разработанные рекомендации на основе математико-статистического метода экспертных оценок позволят улучшить производство организационных работ по ликвидации аварийных участков теплотрасс и снизить количество аварийных работ, уменьшив при этом заболеваемость работников предприятий теплоснабжения, повысить безопасность труда особенно в осенне-зимний период года, а также сократить экономические потери от ликвидации аварийных ситуаций и лечения заболевших работников теплогенерирующих предприятий.

Результаты. На основании профилактических графиков ремонтных работ можно спланировать первоочередность замены труб аварийных участков, что существенно уменьшит объемы аварийных работ по замене аварийных участков трубопроводов. Наиболее травмоопасными работами являются газосварочные и электросварочные работы соответственно специальностями, их выполняющими, являются газосварщик и электросварщик . Условия их работы эксперты определяют как опасные и вредные.