УДК 004.056:061.68; 004.3.75:061.68

АНАЛІЗ СТОХАСТИЧНИХ ТА ДИНАМІЧНИХ МОДЕЛЕЙ НЕСАНКЦІОНОВАНОГО ДОСТУПУ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ ДЕРЖАВИ

І.Р.Опірський, П.І. Гаранюк, Т.І.Головатий

Національний університет «Львівська політехніка»
вул. С.Бандери 12, 79013, Львів, Україна

Представлено та розроблено систематичну схему проблем моделювання процесів несанкціонованого доступу (НСД) на інформацію та її захист. Проведено аналіз та дослідження стохастичних та динамічних моделей політик безпеки при НСД в інформаційних мережах держави (ІМД) (модель Лукіна-Волокіти, модель «вартість-безпека», модель Кобозєвої-Хорошка , модель Пуассона, модель Ігнатова В.О, нестаціонарна модель системи інформативного обміну процесів захисту об'єктів Пархуця Л.Т., динамічна модель реалізації загроз Язова Ю.К.) .

Визначено, що недоліком моделі Лукіна-Волокіти, що обмежує сферу її застосування, є потреба отримання достатньої статистичної вибірки, за якою формується граф цілей зловмисників, а недоліком застосування динамічної моделі Кобозєвою А.А. та Хорошко В.О. є труднощі отримання в явному аналітичному вигляді моделі процесу нападу на інформацію за допомогою застосування прямих методів.

Дослідження показали, що недоліком моделі Язова Ю.К є громіздкість розрахунків, що значно ускладнює її цільове застосування на практиці, а перевагою є – можливість отримання області кількісних оцінок можливостей реалізації загроз у комп'ютерних мережах з урахуванням фактору часу, чим досягається ґрунтовне підвищення вимог до заходів, що проводяться з метою захисту інформації.

Ключові слова: *несанкціонований доступ, стохастичні моделі захисту, динамічні моделі захисту, модель захисту, модель Лукіна-Волокіти, модель «вартість-безпека», модель Кобозєвої-Хорошка, модель Пуассона, модель Ігнатова В.О, нестаціонарна модель системи інформативного обміну процесів захисту об'єктів Пархуця Л.Т., динамічна модель реалізації загроз Язова Ю.К.*

Постановка проблеми. Глобальне використання персональної електронообчислювальної машини (ПЕОМ) та інформаційно-телкомунікаційні системи (ІТС) практично в усіх сферах життєдіяльності суспільства відкрила можливість масового доступу користувачів і зловмисників до інформації. У зв'язку з цим, на перший план виходить і активізується проблема створення високоефективних системи протидії та захисту (СПЗ).

Теоретичне підгрунтя для створення сучасних СПЗ виступають політика безпеки й моделі безпеки, які відображають процеси НСД на інформацію та регулюють механізми її захисту. Під політикою безпеки розуміють інтегральну і, як правило, якісну характеристику, що описує властивості, принципи та правила

захищеності інформації в ІМД в загальному просторі загроз. Модель безпеки являє собою формалізоване (математичне, аморетмічне, схемотехнічне тощо) подання обраної політики безпеки. Головним призначенням моделей безпеки є вибір та обґрунтування базисних принципів архітектури, що визначають механізми реалізації засобів захисту інформації, підтвердження властивостей (наприклад, рівня захищеності інформації) системи, яка розробляється шляхом формального доведення дотримання політики безпеки, складання формальної специфікації політики безпеки новостворювальної СПЗ, тощо. Узагальнивши відомі підходи, подамо систематичну схему проблеми моделювання процесів НСД (стан нападу) на інформацію та її захисту (рис. 1), виходячи з неї, дослідимо та проаналізуємо існуючі моделі.

Як видно з рис.1 систематика досліджувальної проблеми визначає, власне, і сучасну технологію моделювання процесів нападу на інформацію та її захисту.

Для моделювання процесів НСД з інформацією в ІМД широкого використання набули теоретичні моделі безпеки.

Так основною теоретичного підходу є методи теорії підтримки та прийняття рішень, теорії графів, теорії ймовірностей та напівмаркованих процесів тощо. Розроблені на їх базі відповідні моделі (рис. 1) в основному відкривають можливість отримання якісних оцінок рівня захищеності інформації.

Синтез теоретичного та емпіричного підходів (див. рис. 1) ґрунтується на групі математичних методів, які відносяться до них.

Детально проаналізуємо лише ті стохастичні та динамічні моделі, які отримані найбільше розповсюдження.

Аналіз останніх досліджень та публікацій. Аналізом та дослідженням загальних моделей несанкціонованого доступу в інформаційних мережах держави займались відомі вчені та науковці світу. Так, наприклад, у наукових працях, авторами яких є: Воробйов А.А.[1], Мельников В.В.[2],Щербаков А.Ю, Дев'янін П.Н., Габович А.Г., Петренко С.А., Цирлов В.Л.[3],Браїловський М.М.[4], Габович А.Г., Горобець А.Ю., Махальський О.О. тощо прийнято дотримуватися такої класифікації відповідних політик й моделей безпеки:

- моделі дискретного доступу (модель Хартсона, модель Хартсона-Рузо-Ульмана; модель TAM; модель TAKE-GRANT тощо);
- моделі мандатного доступу (модель Бела-Лападулі, модель Low-WaterMark тощо);
- моделі математичного доступу;
- моделі рольового доступу (модель Лендвера і Мак-Ліна);
- автоматичні та теоретично-імовірністні моделі (Гогена-Медигера);
- моделі контролю цілісності (модель Біба, модель Кларка-Вілсона);
- модель захисту від загроз відмов в обслуговуванні (модель Мілена) тощо.

Зважаючи на вище наведену класифікацію відомих політик та моделей, на практиці вимагається можливість розкриття суті базових підходів, які покладено в їх основу. Крім того, за самої класифікації ускладнюється науково-технічний аналіз математичного базису моделей.

Існує й інший, альтернативний, підхід до класифікації моделей, якого дотримуютья переважно вітчизняні вчені – Кобозєва А.А., Андрєєв В.І., Козлов В.С., Хорошко В.А., [5], Козлова К.В., Пархуць Л.Т., Горбенко І.Д., Кавун С.В.[6]. В основу їх класифікації покладено теоретичний, емпіричний та теортико-емпіричний підходи.

Для моделювання процесів НСД з інформацією в ІМД широкого використання набули теоретичні моделі безпеки, які досить докладно описані в [7-11].

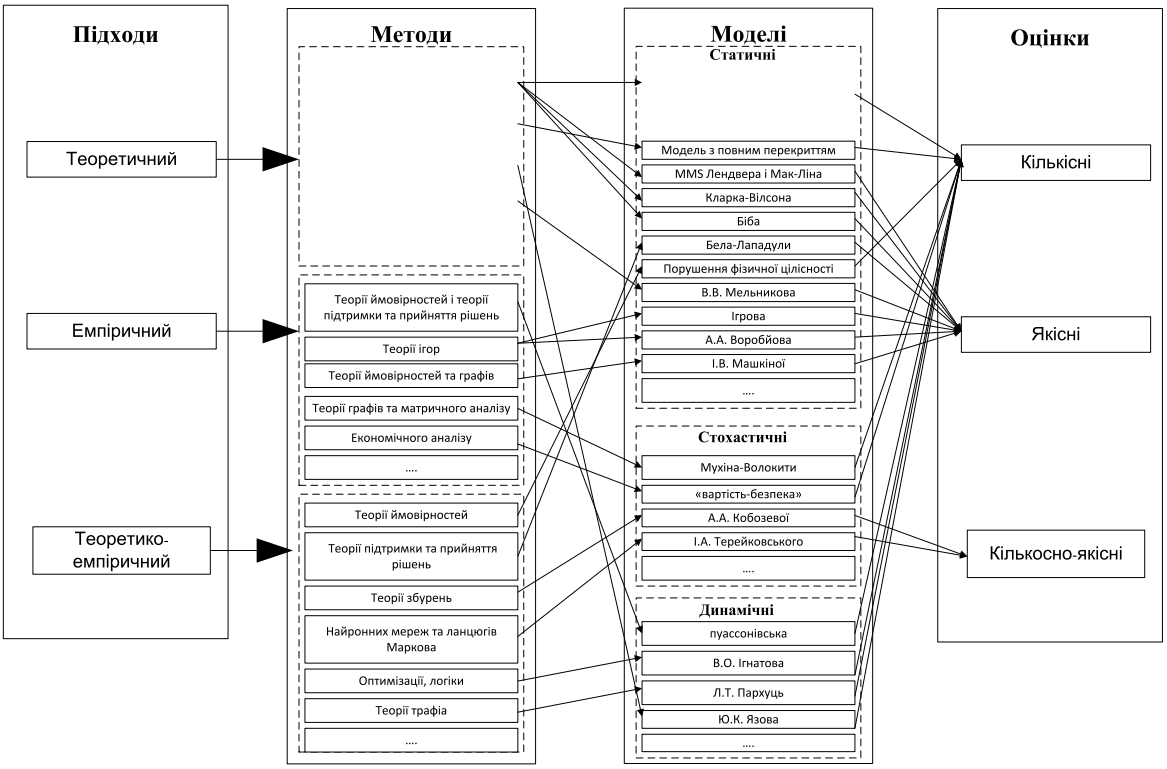

Рис.1. Схема проблем моделювання процесів НСД на інформацію та її захисту

Мета статті. Розроблення на основі аналізу сучасних методів та моделей політик та безпеки систематичної схеми проблем моделювання процесів НСД (стан нападу) на інформацію та на основі неї проведення детального аналізу та дослідження стохастичних та динамічних моделей політик безпеки при НСД в ІМД (модель Лукіна-Волокіти, модель «вартість-безпека», модель Кобозєвої-Хорошка, модель Пуассона, модель Ігнатова В.О, нестаціонарна модель системи інформативного обміну процесів захисту об'єктів Пархуця Л.Т., динамічна модель реалізації загроз Язова Ю.К.), які отримали найбільше розповсюдження при моделюванні процесів НСД та при створенні СПЗ від НСД в ІМД на предмет їх переваг та недоліків.

Виклад основного матеріалу дослідження. В основу переважної кількості відомих стохастичних моделей покладено емпіричний та теоретико-емпіричний підходи, оскільки їх основною виступають статичні ймовірності, розраховані на основі відомої статистики ймовірностей реалізації НСД на типових об'єктах інформатизації та ІТС на заданому часовому інтервалі спостереження.

Моделювання процесів НСД щодо інформації за моделлю Лукіна-Волокіти, яка відноситься до даної групи моделей, полягає у графові-матричному аналізі досягнення цілей зловмисником щодо здійснення НСД до інформації.

Вихідними даними для моделювання виступає сеансовий вектор X, що являє собою лічильник факторів різних загроз безпеці інформації x_i, що зафіксовано засобами збору та перевірки стану системи, тобто:

$$X = \{x_1, x_2, \ldots, x_n\}. \quad (1)$$

Несанкціонований доступ до інформації описується за допомогою вагової матриці коефіцієнтів АХ:

$$AX = \begin{bmatrix} ax_{11} & \cdots & ax_{1m} \\ \vdots & \ddots & \vdots \\ ax_{n1} & \ldots & ax_{nm} \end{bmatrix}, \quad (2)$$

де ax_{ij} - коефіцієнти матриці, що показують величину відповідного фактора x_i у кінцевій дії a_j зловмисника.

Елементи вектора А a_j розраховуються як:

$$a_j = \sum_{i=1}^{n} x_i ax_{ij} . \quad (3)$$

Для формування вектора досягнення цілей G= $\{g_1, g_2, \ldots, g_k\}$, де g_i – локальна ціль зловмисника, яким формується вагова матриця GA.

$$GA = \begin{bmatrix} ga_{11} & \cdots & ga_{1m} \\ \vdots & \ddots & \vdots \\ ga_{n1} & \cdots & ga_{nm} \end{bmatrix}, \quad (4)$$

елементи якої ga_{ij} розраховують як:

$$g_j = \sum_{i=1}^{n} a_i ga_{ij}, \quad (5)$$

У результаті диференціальна оцінка ймовірності НСД P_i визначається як ймовірність досягнення зловмисником локальної цілі g_i з урахуванням коефіцієнта нормування $k_j \in [0,1]$, тобто

$$g_j = \sum_{i=1}^{n} a_i ga_{ij}. \quad (6)$$

Наступним етапом моделювання є формування графа цілей зловмисників на основі статистичного набору даних про події в системі. Вершини графа =описують цілі зловмисників, дуги – дії, що сприяють переходу від однієї до іншої цілі.

До переваг даної моделі відноситься підвищення, порівняно із відомими, ймовірність коректного виявлення НСД, що дозволяє оперативно й адекватно локалізувати та реагувати на нього.

Головним недоліком даної моделі, що обмежує сферу її застосування, є потреба отримання достатньої статистичної вибірки, за якою формується граф цілей зловмисників. Якість вхідних даних носить суб'єктивний характер, що

визначається рівнем кваліфікації та підготовленості експертів, які залучаються для опитування та оцінювання відповідно до обраних методів, які застосовуються для обробки експертної інформації.

Модель «вартість-безпека» відноситься до класу економічних моделей, що оптимізують збитки від нападу на інформацію та затрати на її захист.

У моделі «вартість-безпека» передбачається, що витрати В, які забезпечують необхідний рівень захищеності інформації, виражаються функціоналом

$$B = F\left[\{R\}, f(R), f(b_r)\right], \tag{7}$$

де {R} – множина можливих загроз інформації, $r \in R$;
$f(R)$ – функція потенційної небезпеки від реалізації загроз R ;
$f(b_r)$ – функція витрат, необхідних для нейтралізації r-ї загрози.

Недоліки даної моделі проявляються на етапі формування статистики, що визначає частоту виникнення відповідних загроз R. Для визначення таких коефіцієнтів, як і в попередній моделі, залучаються експертні оцінки. Як показує аналіз даної моделі, вона має досить наближений характер. Підвищення її адекватності може досягтися лише підвищенням складності аналітичних викладок, в основі яких повинні лежати теорія ймовірності і теорія підтримки та прийняття рішень

У монографії вперше для аналізу інформаційної безпеки, процесів та властивостей інформаційних об'єктів застосовано теорію збурень.

Процес нападу на інформацію за моделлю Кобозєвої-Хорошка як частинний випадок інформаційного процесу в ІТС, являє собою деяку неперервну або дискретну вектор-функцію кінцевого числа змінних загального вигляду.

$$\phi\{x_1 \ldots, x_n\} = \begin{pmatrix} \varphi_1(x_1 \ldots, x_n) \\ \varphi_1(x_1 \ldots, x_n) \\ \vdots \\ \varphi_1(x_1 \ldots, x_n) \end{pmatrix} = \begin{pmatrix} \varphi_1 \\ \varphi_2 \\ \vdots \\ \varphi_m \end{pmatrix}, \tag{8}$$

де $(\varphi_1, \varphi_2, \ldots, \varphi_m) \in R^m$– вихідні параметри;
$(x_1 \ldots, x_n) \in D(\varphi) \subseteq R^m$– вихідні параметри $D(\varphi)$ – область визначення функції $(\varphi_1, \varphi_2, \ldots, \varphi_m)$.

Особливість моделювання процесів нападу на інформацію за запропонованою моделлю (1.9) є потреба у формалізації кожної конкретної системи захисту інформації (СЗІ) та тих інформаційних атак, яким вона повинна протистояти. Формалізація процесів нападу на інформацію є досить проблематичним питанням, яке на сьогоднішній день не до кінця опрацьоване і досліджене.

Перевагою запропонованого Кобозєвою А.А. та Хорошко В.О. підходу є можливість моделювання інформаційних процесів тільки статичної природи, де вхідні параметри визначаються набором статистики за експериментальними даними або результатами вимірювань вхідних величин, а й можливість

формалізації динамічної моделі захищеної ІТС. Але недоліком застосування динамічної моделі є труднощі отримання в явному аналітичному вигляді моделі процесу нападу на інформацію за допомогою затосування прямих методів.

Динамічні моделі. На сьогоднішній день найбільш розповсюдженими динамічними моделями є модель Пуассона, модель оптимального управління інформаційною безпекою В.О. Ігнатова, нестаціонарна модель Пархуця Л.Т. , динамічна модель Язова Ю.К. (див.мал.1) тощо.

Найбільш загальний опис динаміки процесу нападу описує модель Пуассона .

При цьому передбачається, що НСД щодо інформації є потоком, який періодично потворюється. Функція розподілу Пуассона загального вигляду $P\left(\bar{\tau} = \frac{\tau}{\lambda}\right)$ визначає ймовірність успішної атаки на ІТС по j-му каналу, в результаті чого відбудеться НСД до інформації τ разів, тобто

$$P\left(\bar{\tau} = \frac{\tau}{\lambda}\right) = \frac{(\lambda t)^{\tau}}{\tau!} e^{-\lambda t}, \qquad (9)$$

де λ – середній коефіцієнт можливої появи загрози певного типу, який у загальному випадку розглядається як нова зміна $\bar{\lambda}$;

τ – кількість проявів загрози за фіксований час, $\tau = 0,1,2,...;$

t – кількість періодів часу за які визначено τ.

Дану модель не можна застосовувати для розв'язання широкого кола задач інформаційної безпеки через відсутність достатньої кількості фактичних даних про прояви загроз та їх наслідків. З цієї причини широкого застосування не знайшли моделі нападу на інформацію, розроблені на базі моделі Пуассона.

Вперше в галузі захисту інформації Ігнатовим В.О. запропоновано подати процес управління інформаційною безпекою у вигляді системи диференціально-логічних рівнянь, що описують динаміку інформаційних конфліктів в системах. Методика моделювання динаміки інформаційних конфліктів за Ігнатовим В.О. має чотирирівневу структуру: формування проблемної області; розробка вербальної моделі; пошук методів вирішення проблеми; пошук оптимальних рішень управління інформаційною безпекою.

Модель Ігнатова В.О. дозволяє враховувати антагонізм інтересів суб'єктів інформаційного конфлікту, але задача моделювання звужується за рахунок розв'язання її лише у позиції теорії оптимального управління. У такій постановці відсутні можливості раціональної організації розподілу інформаційних ресурсів, що виділено на захист інформації, оскільки відомо, що реальні конфлікти в ІТС характеризуються теоретико-ігровими та ймовірнісними властивостями, як і в моделях не досліджені.

Нестаціонарна модель системи інформативного обміну процесів захисту об'єктів Пархуця Л.Т. зводиться до того, що нестаціонарна природа (G) процесу нападу

на інформацію (I) з нестаціонарною зміною (Θ) рівня захищеності (W) технічного об'єкта (TO) в ІТС описується $G|\Theta W$ моделлю з відповідними ймовірностями характеристиками об'єкта при перебуванні ним у різних інформаційних станах.

$G|\Theta W$ модель процесу нападу на інформацію подано як імовірність відмови системи інформаційного обміну від часу, тобто

$$P(t) = 1 - \exp\left[-\sum\nolimits_j \int\nolimits_{\tau_{ij} \in T} \Lambda_i(t) dt \right], \qquad (10)$$

де $\Lambda_i(t)$ – інтенсивність атак при переході системи в і-й стан.

На застосування підходу до моделювання процесу нападу на інформацію з деякою кількістю інформаційних станів, що перевищує в ІТС, накладається обмеження через значне ускладнення аналітичних випадків.

Динамічна модель реалізації загроз Язова Ю.К. ґрунтується на використанні математичного апарату мереж Петрі-Маркова. Мережі Петрі в даній моделі застосовуються для моделювання атак, а ланцюги Маркова – для характеристики часових та стохастичних параметрів моделі та для опису вектора ймовірностей станів системи.

Динаміка реалізації загрози в моделі являє собою послідовність переміщень, що реалізовані у вигляді напівкроків по мережі Петрі-Маркова, при цьому передбачається, що мережа перебуває у кожному із визначених станів певний час. В аналітичний формі процес описується інтеро-диференціальними рівняннями за траєкторіями переміщень із початкового у кінцевий термінальний стан.

Недоліки моделі Язова Ю.К є громіздкість розрахунків, що значно ускладнює її цільове застосування на практиці.

Перевагою моделі є можливість отримання області кількісних оцінок можливостей реалізації загроз у комп'ютерних мережах з урахуванням фактору часу, чим досягається ґрунтовне підвищення вимог до заходів, що проводяться з метою захисту інформації.

Висновки. Отже, з наведеного вище науково-технічного аналізу випливає однозначний висновок:

- розвиток кількісної методології оцінювання рівня захищеності інформації від методів НСД є однією із кардинальних проблем теорії захисту інформації;
- отримання кількісних оцінок рівня захищеності інформації від методів НСД має безпосередній зв›язок із аналітичним або імітаційним моделюванням;
- розробка кількісного підходу пов'язана з вирішенням ряду проблем, серед яких головними є розробка формалізованих моделей процесів нападу на інформацію з нелінійною та нестаціонарною природою, а також розробка шкали кількісного оцінювання за розробленими методами тощо;
- розробка перспективних високоефективних СЗІ та СПЗ на базі динамічних моделей потребує розробки аналітичних моделей процесів нападу на інформацію, які підлягають всебічному систематичному аналізу.

Список використаних джерел

1. Воробьев А.А. Оценивание защищённости автоматизированных систем на основе методов теории игр/ Воробьеов А.А., Куликов Г.В., Некомнящих А.В.// – Информационные технологии.–М: Новые технологии, 2007.-24с.
2. Мельников В.В. Безопастность информации в автоматизированных системах/ Мельников В.В.–М: Финансы и статистики, 2003.–368с.
3. Цирлов В.Л. Основы информационной безопастности автоматизированных систем/ Цирлов В.Л. –М: Феникс,2008.–173с.
4. Браїловський М.М. Технічний захисту інформації на об'єктах інформаційної діяльності/ Браїловський М.М., Головань С.М., Домарєв В.В.– К: Вид. ДУІКТ, 2007.–178с.
5. Габович А.Г. Методика оцінки рівня безпеки інформації/ Габович А.Г., Горобець А.Ю., Хорошко В.О.// Вісник НУ «ЛП» –№55,2006.– С.46-53.
6. Кавун С.В. Математичне моделювання процесів побудови параметрів еліптичних кривих для криптографічних перетворень / І. Д. Горбенко, О. Є. Ілясова // Радіоелектронні і комп'ютерні системи. - 2006. - № 5. - С. 103–107.
7. Згуровський М.З. Основи системного аналізу/ Згуровський М.З., Панкратова Н.Д.– К:BHV, 2007. –544с.
8. Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорії диференціальних ігор та диференціальних перетворень – Житомир:Рута.–2010.–280с.
9. Brumnik, R., Klebanova, T., Guryanova, L., Kavun, S., Trydid, O. (2014). Simulation of Territorial Development Based on Fiscal Policy Tools, Mathematical Problems in Engineering, vol. 2014, Article ID 843976, 14 pages, 2014. doi:10.1155/2014/843976.
10. Information technology security evaluation criteria. Harmonized criteria of France-Germany-the Netherlands-the United Kingdom–Department of Trade and Industry, London,1991.
11. ISO 15408 The Common Criteria for Information Technology Security Evaluation.–2005.
12. Kavun, S., Mykhalchuk, I., Kalashnykova, N., Zyma, A. (2012). A Method of Internet-Analysis by the Tools of Graph Theory. En: Watada, J., Phillips-Wren, G., Jain, L.C., and Howlett, R.J. (Eds.), Advances in Intelligent Decision Technologies, SpringerVerlag Series "Smart Innovation, Systems and Technologies", Vol. 15, Part 1, Heidelber, Germany, pp. 35-44, DOI: 10.1007/978-3- 642-29977-3_4.

References

1. Vorob'eov A.A., Kulykov H.V. & Nekomnyashchykh A.V.(2007). Otsenyvanye zashchyshchennosty avtomatyzyrovannukh system na osnove metodov teoryy igr. Informatsyonnue tekhnolohyy.Moskva: Novue tekhnolohyy, 24. (in Russian)
2. Mel'nykov V.V.(2003). Bezopastnost' informatsyy v avtomatyzyrovannukh systemakh. Moskva: Fynansu i statystyky, 368. (in Russian)
3. Tsyrlov V.L.(2008). Osnovu informatsyonnoy bezopastnosty avtomatyzyrovannukh system. Moskva: Fenyks, 173. (in Russian)
4. Brayilovs`ky`j M.M. (2007). Tekhnichny`j zakhy`stu informaciyi na ob'yektakh informacijnoyi diyal`nosti/ Brayilovs`ky`j M.M., Golovan` S.M., Domaryev V.V.– K: Vy`d. DUIKT,178s. (in Ukrainian)
5. Habovych A.H., Horobets' A.Yu. & Khoroshko V.O.(2006). Metodyka otsinky rivnya bezpeky informatsiyi. Visnyk NU «LP», № 55, 46-53. (in Ukrainian)

6. Kavun S.V. (2006). Matematy`chne modelyuvannya procesiv pobudovy` parametriv elipty`chny`kh kry`vy`kh dlya kry`ptografichny`kh peretvoren` / I. D. Gorbenko, O. Ye. Ilyasova // Radioelektronni i komp'yuterni sy`stemy`. - - # 5. - S. 103–107. (in Ukrainian)
7. Zgurovs`ky`j M.Z. (2007). Osnovy` sy`stemnogo analizu/ Zgurovs`ky`j M.Z., Pankratova N.D.– K:BHV, 544s. (in Ukrainian)
8. Gry`shhuk R.V. (2010). Teorety`chni osnovy` modelyuvannya procesiv napadu na informaciyu metodamy` teoriyi dy`ferencial`ny`kh igor ta dy`ferencial`ny`kh peretvoren` –Zhy`tomy`r:Ruta.—280s. (in Ukrainian)
9. Brumnik, R., Klebanova, T., Guryanova, L., Kavun, S., Trydid, O. (2014). Simulation of Territorial Development Based on Fiscal Policy Tools, Mathematical Problems in Engineering, vol. 2014, Article ID 843976, 14 pages, 2014. doi:10.1155/2014/843976. (in English)
10. Information technology security evaluation criteria. Harmonized criteria of France-Germany-the Netherlands-the United Kingdom–Department of Trade and Industry (1991). London. (in English)
11. ISO 15408 The Common Criteria for Information Technology Security Evaluation. (2005). (in English)
12. Kavun, S., Mykhalchuk, I., Kalashnykova, N., Zyma, A. (2012). A Method of Internet-Analysis by the Tools of Graph Theory. En: Watada, J., Phillips-Wren, G., Jain, L.C., and Howlett, R.J. (Eds.), Advances in Intelligent Decision Technologies, SpringerVerlag Series "Smart Innovation, Systems and Technologies", Vol. 15, Part 1, Heidelber, Germany, pp. 35-44, DOI: 10.1007/978-3- 642-29977-3_4. (in English)

ANALYSIS OF STOCHASTIC AND DYNAMIC MODELS OF UNAUTHORIZED ACCESS TO STATE INFORMATION NETWORKS

I.R. Opirskyy, P.I. Garanyuk, T.I. Holovatyj

Lviv Polytechnic National University
12, Bandera St., Lviv 79013, Ukraine
e-mail: garanyuk@gmail.com

The authors have presented and developed a systematic scheme of modeling problems of unauthorized access (UA) to the information and its protection. The analysis and the study of stochastic and dynamic models of security policies at UA in state information networks (SIN) (Lukin-Volokita model, the model "cost-security", Kobozyeva-Khoroshko model, Poisson model, Ihnatov model, a non-stationary model of informative exchange of security object processes by Parkhuts L.T., a dynamic model of threats implementation by Yazov Yu.K.) have been done.

It has been determined that the disadvantage of the model of Volokita-Lukin, limiting its scope, is the need to obtain sufficient statistical sampling, on which we build the graph of criminal purposes, and the disadvantage of the application of the dynamic model of Kobozeva and Khoroshko is the difficulty of obtaining a model of attack process on the information in explicit analytic form through the use of direct methods.

Researchers have shown that the lack of Yazov model is cumbersome calculations, which greatly complicate its intended application in practice, and the advantage is the possibility of quantitative field assessments of the feasibility of threats in computer networks, taking into account the time factor, thus achieving thorough increasing demands to the measures undertaken to protect the information.

Keywords: *unauthorized access, stochastic security model, dynamic security model, security model, Lukin-Volokita model, model "cost-security", Kobozyeva-Khoroshko model, Poisson model, Ihnatov model, non-stationary model of the system of informative exchange of security object processes by Parkhuts L.T., dynamic model of threats implementation by Yazov Yu.K.*

Стаття надійшла до редакції 20.03.2016.
Received 20.03.2016.