УДК 004.056:323.1
Хусаінов П.В. (ВІТІ)

ПОКАЗНИК КІБЕРНЕТИЧНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНОЇ СИСТЕМИ У ЧАСІ

Стаття містить викладення деяких принципів, результатів дослідження проблематики кібернетичної безпеки автоматизованої системи у часі. Запропонований показник кібернетичної безпеки автоматизованої системи адитивного виду. Він складається з низки ймовірнісних показників експонентного закону розподілу, стаціонарного граничного стану ланцюга Маркова і своєчасного прийняття рішення. Також були використані нормалізовані показники величини можливої шкоди внаслідок комп'ютерної атаки.

Хусаинов П.В. Показатель кибернетической безопасности автоматизированной системы во времени. *Статья содержит изложение некоторых принципов, результатов исследования проблематики кибернетической безопасности автоматизированной системы во времени. Предложен показатель кибернетической безопасности автоматизированной системы аддитивного вида. Он включает ряд вероятностных показателей экспоненциального закона распределения, стационарного предельного состояния цепи Маркова и своевременного принятия решений. Также были использованы нормализированные показатели величины возможного ущерба вследствие компьютерной атаки.*

P. Khusainov Coefficient automated system's cybersecurity in the time. *The paper constitutes the statement some principles, results of an investigation into automated system's cybersecurity in the time. Additional coefficient of automated system's cybersecurity is presented. Its coefficient include probable indexes of exponential distribution law, Markov's chain stationary state and on-line decision making. The normalized indicators of potential damage on the computer's attack were also used.*

Ключові слова: *загрози безпеці інформації кібернетичної природи.*

Вступ

На початку 90-х р.р. XX ст. теоретико-методологічний базис військового мистецтва збагатився новим напрямом досліджень шляхів здобуття переваги, перемоги над високотехнологічним противником застосовуючи узгоджені за місцем і часом сукупність методів, способів та прийомів інформаційно-психологічного впливу, погіршення якості і безпеки інформаційних процесів, більш оперативного збирання та аналізу розвідувальної інформації, радіоелектронного придушення, руйнування технічних засобів обміну даними і т. ін. [1].

Згодом стало очевидним, що масовий характер потенційно-небезпечних дефектів проектування та реалізації програмного забезпечення (до 5 шт. на 1000 рядків початкового коду) автоматизованих інформаційних систем обумовлює значні перспективи розробки методів, способів, засобів, так званої, ,,кібернетичної зброї", особливо, якщо обчислювальне середовище об'єкта руйнівного кібернетичного впливу утворює ОС загального призначення [2 – 4].

Невдовзі (початок 2000-х р.р.) тематика ,,інформаційних війн" (від англ. – *information and psychological warfare*) почала активно обговорюватися в наукових колах нашої країни, але переважно у воєнно-прикладному аспекті її інформаційно-психологічної складової. Результат досить тривалого, так би мовити наївного періоду, за Д. Гільбертом, втілення у життя будь-якої нової теорії, призвів до появи організаційних структур з відповідними цілями, задачами і функціями, термінології щодо інформаційної безпеки держави у воєнній сфері [5].

Одночасно, разом з завершенням узгодження і прийняттям більш менш загальноприйнятого, консенсусного варіанту ,,термінологічних баталій", стала очевидною фактична відсутність суттєвих наукових результатів, які б дозволили перейти до практичного вирішення задач аналізу і синтезу систем захисту від ,,кібернетичної зброї".

Аналіз останніх публікацій

Згідно нормативних документів технічного захисту інформації (НД ТЗІ) забезпечення захисту інформації в автоматизованій системі (АС) базується на створенні і застосуванні комплексної системи захисту інформації (КСЗІ) в якій, одним з обов'язкових елементів,

поряд із сукупністю організаційних і інженерних заходів, є програмно-апаратний комплекс засобів захисту (КЗЗ).

Основним завданням КЗЗ є реалізація того чи іншого варіанту концепції диспетчера доступу, яка полягає у забезпеченні контролю всіх запитів, що надходять від обчислювальних процесів (суб'єктів) стосовно набуття доступу до об'єктів обчислювального середовища (файлів, каталогів, об'єктів пам'яті, пристроїв і т. ін.) з одночасним прийняттям рішення про допустимість чи заборону такого звертання згідно правил розмежування доступу (ПРД) як ключової частини політики безпеки АС [6].

Теоретичним базисом [7 – 8] концепції диспетчера доступу стала суб'єктно-об'єктна методологія дослідження програмно-технічних систем розвинута ідеєю про перебування системи у безпечному стані, якщо суб'єкти не можуть порушувати ПРД. Її основні положення:

- система – сукупність взаємодіючих суттєвостей суб'єктів та об'єктів;
- взаємодії в системі моделюються встановленням відношень суб'єктів і об'єктів;
- множина типів відношень визначається як набір операцій суб'єктів над об'єктами;
- сукупність множин суб'єктів, об'єктів та відношень між ними – стан системи;
- безпека системи забезпечується шляхом управління доступом суб'єктів до об'єктів;
- безпека системи у часі може бути цілком забезпечена шляхом управління доступом.

Повною мірою остаточне оформлення теоретичних засад диспетчера доступу відбулося з розробкою на її основі низки формальних моделей більш-менш придатних для логічного доведення теорем про безпеку системи (початок 70-х р.р. – середина 80-х р.р. XX ст.): Харрісона–Руззо–Ульмана, *Take-Grant*, Белла-ЛаПадулла, дискреційної (від англ. – *Discretionary Access Control, DAC*), мандатної (від англ. – *Mandatory Access Control, MAC*) та рольової (від англ. – *Role Base Access Control, RBAC*) політики управління доступом.

На практиці [9] реалізація суб'єктно-об'єктної парадигми забезпечення безпеки інформації АС зводиться до організації розмежування доступу її користувачів до логічних об'єктів обчислювального середовища з якими асоціюються ті чи інші структурні одиниці інформації. Повноваження на доступ до інформаційних об'єктів у тій чи іншій формі успадковуються обчислювальним процесом, так би мовити, лідером ініційованого сеансу роботи фізичного користувача з АС після його успішної авторизації засобами ОС, який, в свою чергу, забезпечує функціонування текстового або графічного користувальницького операційного середовища.

Користувач, виконуючи певні автоматизовані функції у контексті організованої в АС інформаційної технології і звертаючись до того чи іншого об'єкта свого інформаційного домену, кожного разу неявно генерує запит до програмної реалізації диспетчера доступу ядра ОС щодо перевірки відповідності повноважень, атрибутів доступу згідно ПРД. Запуск на виконання користувачем інших програм більш складний ніж читання/запис файлів, але і він зводиться, як правило, до виконання низки запитів до диспетчера доступу ядра ОС щодо визначення правомочності читання системним завантажником з файла, що виконується двійкового коду і даних програми, файлів бібліотек, створення нового, дочірнього обчислювального процесу лідера сеансу з успадкуванням його повноважень, і взагалі, в момент створення кожний новий обчислювальний процес є копією батьківського.

Таким чином, у контексті сеансу роботи авторизованого користувача, особливо, під управлінням ОС загального призначення, утворюється ієрархічне родинне дерево обчислювальних процесів з відповідними рівними повноваженнями, коренем якого є лідер сеансу. Завдяки цьому, при належному функціонуванні диспетчера доступу ядра ОС, сформувалась струнка, наочна картина забезпечення безпеки інформації в АС: користувальницькі обчислювальні процеси ізольовані у межах свого інформаційного домену [10].

Вважається, що у непривілейованого користувача немає можливості розширити (змінити) свої повноваження, тим самим створити необхідні умови для виходу за межі свого

інформаційного домену і порушення ПРД, але якщо така можливість у нього з'явиться, то існує висока ймовірність порушити безпеку інформації АС авторизованим користувачем-порушником завдяки виходу за межі його інформаційного домену не вступаючи в конфлікт з ПРД.

Сучасні ОС загального призначення, реалізуючи концепцію примусової багатозадачності з розділенням часу, що передбачає можливість одночасної присутності в обчислювальному середовищі АС множини обчислювальних процесів, які почерзі, за вказівкою ядра ОС, виконують свій двійковий код протягом часових квантів роботи процесора електронно-обчислювальної машини. Окрім вже згаданих обчислювальних одиниць сеансу роботи авторизованого користувача, інші обчислювальні процеси, як правило, є службовими, призначеними для забезпечення роботи різноманітних функціональних сервісів для інформаційної технології АС у фоні, без прив'язки до будь-якого сеансу.

При цьому основним способом надання тому чи іншому службовому обчислювальному процесу певних повноважень полягає у ініціюванні його виконання при ініціалізації ОС від імені так званого псевдокористувача, що по суті є зручною абстракцією, органічно вплетеною в реалізацію розмежування доступу до об'єктів відповідного службового інформаційного домену [11].

Існування потенційно-небезпечних дефектів проектування та програмної реалізації службових обчислювальних процесів – демонів створюють передумови їх використання як уразливості КСЗІ АС у частині, що базується на застосуванні механізму розмежування доступу. Відомо чимало колекцій [12 – 14] прикладів потенційно-небезпечних дефектів програмних реалізацій поширених службових демонів та опис їх використання, серед них: *Common Vulnerability Enumeration, Common Weakness Enumeration, Common Attack Pattern Enumeration and Classification.*

Наслідки експлуатації потенційно-небезпечних дефектів, як правило, призводять до аварійного завершення обчислювального процесу або до можливості оперування об'єктами його інформаційного домену з відповідними повноваженнями за ініціативою локального чи віддаленого авторизованого користувача-порушника або інсайдера (від англ. *insider* – внутрішній порушник).

Основним програмно-технічним методом захисту АС від ,,кібернетичної зброї" вважається застосування системи виявлення вторгнень (від англ. *Intrusion Detection System, IDS* – система виявлення вторгнень) у складі КЗЗ КСЗІ АС. В основу функціонування *IDS* покладено принцип розпізнання і блокування всіх тільки відомих з досвіду спроб використання ,,кібернетичної зброї" за їх характерними формалізованими статичними, динамічними ознаками у обчислювальному середовищі АС як об'єкта кібернетичного впливу під час їх здійснення сформованими в єдину базу [15].

Постановка завдання

Виходячи з викладеного, однією з центральних проблем застосування *IDS*, можна вважати принципове зменшення повноти її бази формалізованих шаблонів (правил, сигнатур) характерних статичних, динамічних ознак у часі.

Метою роботи є оприлюднення основних положень дослідження проблемних питань кібернетичної безпеки в частині, що стосується формалізації кібернетичної безпеки АС у часі, на основі використання показника величини запобігання шкоди, яка, в свою чергу, прив'язана до повноти бази формалізованих шаблонів (правил, сигнатур) характерних ознак відомих *IDS* кібернетичних атак.

Основна частина.

Функціонування АС у часі можна представити як послідовність стрибкоподібних переходів між кінцевою множиною станів у випадкові моменти часу. Завдяки цьому, сума ймовірностей перебування у кожному зі станів функціонування системи у часі дорівнює одиниці. Інтервали між суміжними моментами переходів прийнято називати кроками.

Часовий інтервал перебування у тому чи іншому стані – неперервна випадкова величина, а перехід між станами розглядається як подія. Послідовність переходів між станами обумовлена потоком однотипних подій, які слідують одне за одним у випадкові моменти часу.

Для формалізації поняття кібернетична безпека $\Re(t)$ пропонується:

$$\Re(t) = \sum_l P_l(t) \cdot \Re_l(t), \qquad (1)$$

де $P_l(t)$ – ймовірність l-го стану АС, $\sum_l P_l = 1$; $\Re_l(t)$ – показник кібернетичної безпеки при перебуванні АС у l-му стані. Під кібернетичною безпекою АС будемо розуміти стан АС, в який виключена (мінімізована) можливість виконання непередбаченої політикою безпеки інформації обчислювальної роботи, виходячи з наступних міркувань:

1. На сучасному етапі розвитку теорії захисту інформації основним підходом до забезпечення безпеки інформації в комп'ютеризованих системах є застосування концепції розмежування доступу обчислювальних процесів до інформаційних об'єктів АС у контексті суб'єктно-об'єктної методології розгляду складних програмно-технічних систем. При цьому в якості центрального припущення вважається, що всі обчислювальні процеси не можуть виконувати непередбачену розробниками обчислювальну роботу за межами свого інформаційного домену завдяки якісному функціонуванню диспетчера доступу.

2. В останні десятиріччя стало відомо чимало практичних прикладів реалізації можливості нав'язати одним обчислювальним процесом іншому непередбаченої розробниками обчислювальної роботи. У ході обміну даними, цільовому обчислювальному процесу надаються спеціальним чином сформовані дані, обробка яких, разом із забезпеченням необхідних умов може призвести до прояву того чи іншого потенційно-небезпечного дефекту його проектування або програмної реалізації, що у тій чи іншій формі тягне за собою його непередбачену в нормальних умовах поведінку (реакцію), а по суті виконання непередбачених розробниками обчислювальних дій (роботи).

3. З позиції того, що ПРД політики безпеки інформації АС є строго формалізованою основою прийняття рішень диспетчером доступу надання/заборони використання обчислювальним процесом об'єктів як свого інформаційного домену, так і за його межами згідно суб'єктно-об'єктної методології будь-якої базової моделі (дискреційна, мандатна, рольова) забезпечення безпеки інформації у комп'ютеризованій системі. Повноваження обчислювального процесу щодо доступу успадковуються від батьківського при створенні.

4. Відомо, що повноваження службових обчислювальних процесів встановлюються під час їх запуску у ході ініціалізації обчислювального середовища АС і асоціюється з ролями, так би мовити, віртуальними образами псевдокористувачів. Повноваження інших (користувальницьких) – за результатом процедури авторизації користувача як фізичної особи. При цьому, якщо поведінка службових обчислювальних процесів цілком передбачена у часі за умови систематичної і якісної організації адміністративним персоналом АС заходів регламенту системного програмного забезпечення (контроль версій, оновлення, контролю цілісності), то у контексті сеансу фізичного користувача таке припущення не є некоректним.

5. Будь-який непривілейований авторизований локальний чи віддалений користувач в будь-який момент часу може розпочати цілеспрямовану зловмисну діяльність порушника безпеки інформації АС із застосуванням програмних засобів як штатних, так і спеціальних, розроблених з метою використання потенційно-небезпечних дефектів проектування та реалізації працюючих в обчислювальному середовищі АС процесів для виконання ними непередбачених розробниками обчислювальних дій (роботи).

У практичному плані це призводить до виконання того чи іншого варіанту дій щодо оперування об'єктами у інформаційному домені цільового обчислювального процесу за ініціативою непривілейованого авторизованого користувача АС який спрямував зусилля на негативний прояв потенційно-небезпечного дефекту. При цьому ми можемо спостерігати

коректне у теоретичному плані явище: порушення політики безпеки АС, без порушення ПРД і логіки функціонування диспетчера доступу, так би мовити, безконфліктний несанкціонований доступ.

6. У контексті існуючих положень, термінології НД ТЗІ щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу будемо вважати, що загрози безпеці інформації, які передбачають нав'язування обчислювальним процесам АС непередбаченої розробниками обчислювальної роботи на основі використання потенційно-небезпечних дефектів їх проектування та програмної реалізації мають кібернетичну природу. Спробу реалізації загрози безпеці інформації кібернетичної природи АС пропонується називати кібернетичною атакою.

7. Забезпечення захисту АС від загроз безпеці інформації кібернетичної природи обумовлює необхідність розв'язання сукупності взаємопов'язаних, характерних питань від удосконалення (розвитку) існуючої термінології до дослідження (створення) теоретико-методологічної бази придатної для вирішення практичних задач аналізу і синтезу систем кібернетичного захисту.

8. Одним з ключових питань організації ефективного захисту від загроз кібернетичної природи є повнота формалізованої бази шаблонів (правил, сигнатур) відомих кібернетичних атак засобів виявлення (блокування) кібернетичних атак у складі КЗЗ КСЗІ АС, тобто здатність виявити і блокувати всі відомі спроби використання потенційно-небезпечних дефектів проектування та програмної реалізації працюючих в АС обчислювальних процесів.

9. Природа цієї неповноти полягає, по-перше, у практично нескінченній кількості варіантів застосування відомих, вузькоспеціальних формальних знакових систем (мови програмування) для нового викладення будь-якого відомого спеціального алгоритму кібернетичної атаки. По-друге, винаходом нових способів застосування відомих методів, у тому числі, нових варіантів комбінування, удосконалення, об'єднання відомих методів і способів і т. ін. для конкретної кібернетичної атаки. Враховуючи певну недосконаліть математичного апарату теорії розпізнання образів в *IDS* на сучасному етапі пізнання, основним підходом до усунення (зменшення) негативного впливу неповноти залишається систематичне оновлення бази формалізованих шаблонів (правил, сигнатур) тобто додавання нових знань про статичні, динамічні характерні ознаки кібернетичних атак, що стали відомі.

10. Взагалі, справедливо припустити, що своєчасне виявлення і блокування кожної кібернетичної атаки дозволяє запобігти шкоди безпеці інформації АС певної величини, але з часом можуть з'являтися нові реалізації кібернетичних атак проти яких засоби виявлення (блокування) безсилі і не можуть забезпечити автоматичне запобігання шкоди.

Виходячи з викладеного, показник кібернетичної безпеки $\Re_l(t)$ у l-му стані функціонування АС пропонується асоціювати з величиною запобігання шкоди [16] у цьому стані $\Re_l(t) \equiv V_l$, завдяки своєчасному виявленні і блокуванню кібернетичних атак:

$$\Re_l(t) \equiv V_l = W_l - \sum_{k=1}^{|N|} P_k^l(t) \cdot d_k^l \cdot P_{dem}^k(t), \qquad (2)$$

де W_l – показник величини запобігання шкоди, яка досягається завдяки виявленню і блокуванню відомих кібернетичних атак у l-му стані функціонування АС; P_k^l – ймовірність появи нової k-ї кібернетичної атаки у l-му стані функціонування АС; d_k^l – нормований показник величини шкоди, яку може спричинити з ймовірністю $P_{dem}^k(t)$ нова k-ї кібернетична атака у l-му стані функціонування АС, $\sum_{k=1}^{|N|} d_k^l = 1$, $k = \overline{1, |N|}$; N – множина нових кібернетичних атак у l-му стані функціонування АС.

Величина запобігання шкоди W_l, що забезпечується виявленням і блокуванням відомих кібернетичних атак у l-му стані функціонування АС:

$$W_l = \sum_{i=1}^{|A|} \sum_{j=1}^{|G|} \chi_{ij} \cdot w_{ij} \,, \tag{3}$$

де χ_{ij} – оператор розпізнання приналежності (виявлення) i-ї кібернетичної атаки j-му класу наслідків щодо величини можливої шкоди та її миттєвого блокування в момент її розпізнання (виявлення), коли $\chi_{ij} = 1$ і $\chi_{ij} = 0$ – у протилежному випадку; w_{ij} – показник нормованого значення величини запобігання шкоди у l-му стані функціонування АС визначеної на підставі розпізнання приналежності i-ї кібернетичної атаки j-му класу наслідків $\sum_{i=1}^{|A|} \sum_{j=1}^{|G|} w_{ij} = 1$; A – множина відомих кібернетичних атак, які були успішно розпізнані (виявлені) і блоковані у l-му стані функціонування АС, $i = \overline{1, |A|}$; G – множина класів наслідків відомих кібернетичних атак щодо величини можливої шкоди, $j = \overline{1, |G|}$.

Таким чином, кібернетична безпека АС формується з оцінок кібернетичної безпеки у кожному з можливих станів функціонування АС у часі за умови забезпечення повноти формалізованої бази шаблонів (правил, сигнатур) кібернетичних атак:

$$\Re(t) = \sum_{l} P_l(t) \cdot \{W_l - D_l\} = \sum_{l} P_l(t) \cdot \{1 - D_l\}, \tag{4}$$

де $W_l = 1$ – умова повноти формалізованої бази шаблонів (правил, сигнатур) кібернетичних атак в момент переходу до l-го стану функціонування АС; $D_l = \sum_{k=1}^{|N|} P_k^l(t) \cdot d_k^l \cdot P_{dem}^k(t)$ за аналогією (3) виражає величину можливої шкоди, внаслідок відбуття невідомих кібернетичних атак у l-му стані функціонування АС.

На підставі (4) пропонується твердження про те, що величина кібернетичної безпеки у l-му стані функціонування АС є ймовірністю зменшення величини запобігання шкоди завдяки зростанню ймовірності можливої шкоди нових кібернетичних атак у часі, але також з урахуванням ймовірності досягнення кожною з них передбачених практичних наслідків.

Результати дослідження залежності між $P_{dem}^k(t)$ та повнотою досягнення практичних наслідків поширених класів кібернетичних атак у даній роботі не розглядаються.

Для оцінки ймовірності можливої шкоди нових кібернетичних атак у часі пропонується скористатися припущенням про утворення повної групи подій між появою нових кібернетичних атак і зменшенням безпеки обчислювальних процесів АС у часі в умовах цілеспрямованого пошуку та спроб використання потенційно-небезпечних дефектів їх програмної реалізації з метою нав'язування непередбаченої розробниками обчислювальної роботи. Звідси величину $P_k^l(t)$ можна інтерпретувати як ймовірність події, що відомості про характерні ознаки k-ї кібернетичної атаки у l-му стані функціонування АС у формалізованій базі шаблонів (правил, сигнатур) будуть відсутні (рис. 1):

$$P_k^l(t) = 1 - p(t) = 1 - \mathrm{e}^{-\lambda t} \,, \tag{5}$$

де $p(t)$ – ймовірність безпеки обчислювальних процесів АС в умовах потоку спроб (випробувань) використання нових потенційно-небезпечних дефектів їх програмної реалізації з інтенсивністю л .

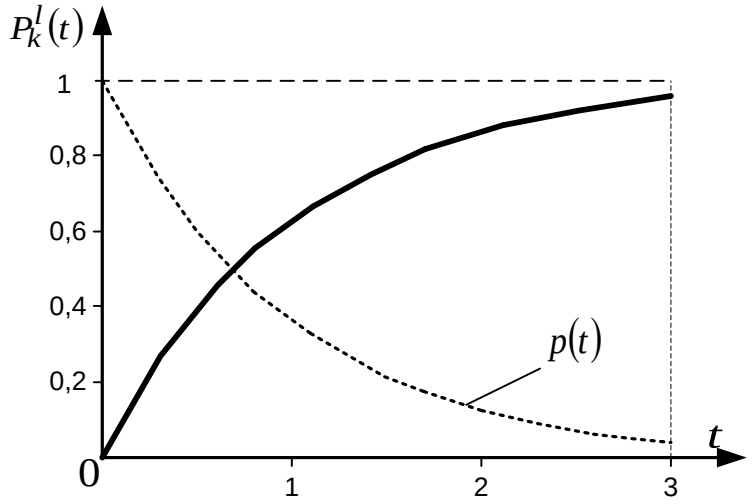

Рис. 1. Залежність $P_k^l(t)$ у часі

Справедливість (5) обумовлена встановленням аналогії між багатоелементним (множина процесів) динамічним обчислювальним середовищем АС випадкової природи і складною технічною системою у термінах теорії надійності, що стосується співвідношень ймовірності відмов та безвідмовної роботи, а також низкою суттєвих позитивних рис [17 – 18]:

1. Експонентний закон розподілу є ідеалізованою моделлю, яка дозволяє при відносно нескладних розрахунках, з деяким наближенням, одержати прості і наочні співвідношення для порівняння різноманітних варіантів вхідних параметрів.

2. При постійній інтенсивності потоку спроб використання нових потенційно-небезпечних дефектів програмної реалізації обчислювальних процесів АС СП ймовірність втрати їх безпеки змінюється за експонентним законом.

3. Постійна інтенсивність потоку за експонентним законом дозволяє справедливо припустити його стаціонарний пуасонівський, найпростіший характер.

4. Ймовірність безпеки обчислювальних процесів АС СП не залежить від моменту відліку часу від першої спроби використання потенційно-небезпечних дефектів їх програмної реалізації, а залежить від інтенсивності цих спроб.

Експонентний розподіл є частковим випадком розподілу Вейбулла при д = 1 з функцією випадкової величини:

$$F_\omega(t,\delta,\sigma,\theta)=\begin{cases}1-\exp\left\{-\left(\dfrac{t-\alpha}{\sigma}\right)^{\delta}\right\} & \text{при } t>0\\ 0 & \text{при } t\le\theta\end{cases}.$$

де д – параметр форми кривої розподілу, у – параметр масштабу, б – параметр зсуву. Суттєвою властивістю розподілу Вейбулла є можливість задати монотонний спад інтенсивності спроб при $д<1$ або їх монотонне зростання – при $д>1$.

Повертаючись до (4), ймовірність спричинення шкоди АС внаслідок здійснення k-ї кібернетичної атаки $P_{dem}^k(t)$ пропонується розглядати у контексті утворення повної групи між цією подією та своєчасним виявленням і блокуванням невідомої кібернетичної атаки адміністративним персоналом із застосуванням наочної інформаційної моделі [19] поточного стану АС з ймовірністю $P_{dm}^k\left(\overline{T}_{dm}\le T_{opt}\right)$:

$$P_{dem}^k(t)=1-P_{dm}^k\left(\overline{T}_{dm}\le T_{opt}\right), \qquad (6)$$

де $\overline{T}_{dm}$ – середній часовий інтервал розпізнання нової кібернетичної атаки за характерними ознаками із застосуванням наочної інформаційної моделі поточного стану АС, вибору та впровадження типового рішення щодо блокування її розвитку у часі (від англ. *decision*

making – прийняття рішень); T_{opt} – обмеження на тривалість $\overline{T}_{dm}$. Результати дослідження залежностей між $P_{dm}^{k}\left(\overline{T}_{dm} \le T_{opt}\right)$, $\overline{T}_{dm}$, T_{opt}, типовими класами наслідків кібернетичних атак та їх основними часовими параметрами у даній роботі не розглядаються.

Для визначення ймовірності перебування АС у l-му стані $P_l(t)$ пропонується розглянути її функціонування у часі, як випадковий процес з дискретними станами і неперервним часом із застосуванням апробованого математичного апарату моделей на основі ланцюгів Маркова, що витікає з низки відомих правил, справедливих для теоретичних припущень:

– потік випадкових подій – найпростіший (стаціонарний, одинарний, без післядії);

– сума потоків випадкових подій з довільними характеристиками при нескінченному збільшенні кількості складових та зменшенні інтенсивності наближається до найпростішого;

– постійна інтенсивність потоків подій у системі говорить про можливість існування граничного стаціонарного режиму;

– у граничному стаціонарному режимі система випадковим чином змінює свої стани, але ймовірність кожного з них не залежить від часу і її можна вважати постійною;

– кінцева кількість станів та можливість перейти в кожний з них за кінцеву кількість кроків обумовлює існування граничних ймовірностей незалежно від початкового стану;

– сума стаціонарних пуасонівських потоків випадкових подій – найпростіший потік;

– випадковий процес у системі буде марковським, якщо всі потоки пуасонівські.

Виходячи з аналізу суттєвих рис функціонування АС у часі, за умови залежності між величиною запобігання шкоди і найпростішим потоком постійної інтенсивності відомих і невідомих кібернетичних атак $P_l(t)$ пропонується розглядати як граничну стаціонарну ймовірність стану S_1, в який переходить система при завершенні чергового оновлення (досягнення повноти) формалізованої бази їх шаблонів (правил, сигнатур) взявши за основу модель Маркова для циклічного випадкового процесу.

Переходи у стани $S_2, \ldots, S_x, \ldots, S_m$, обумовлені найпростішим потоком подій постійної інтенсивності, які відповідають моментам виявлення (блокування) відомих кібернетичних атак, а також моментам виникнення ситуацій розпізнання адміністративним персоналом нової кібернетичної атаки за характерними ознаками із застосуванням наочної інформаційної моделі поточного стану АС (рис. 2).

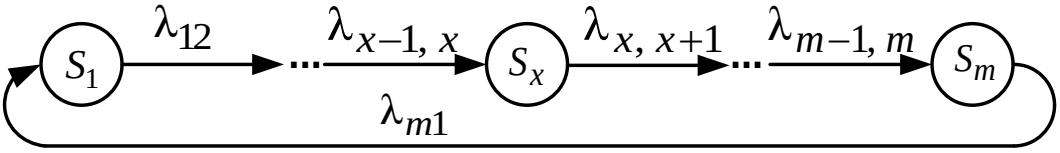

Рис. 2. Розмічений граф випадкового циклічного процесу функціонування АС

Враховуючи органічний зв'язок найпростішого потоку подій зі зворотною експонентному розподілу ймовірності нових кібернетичних атак, і якщо відомі інтенсивності $л_{12}, л_{23}, \ldots, л_{m1}$, то:

$$P_k^l(t) = \frac{1}{1 + \lambda_{12}\left(\frac{1}{\lambda_{23}} + \ldots + \frac{1}{\lambda_{x,\,x+1}} + \ldots + \frac{1}{\lambda_{m1}}\right)}, \qquad (7)$$

де $л_{12} = л_{23} = л_{m-1,m} \equiv л(t)$ – при постійній інтенсивності та експонентному законі розподілу, $m = |A| + |N| - 1$; $л_{m1} = \frac{1}{\overline{T}_{abs}}$ – інтенсивність оновлення (досягнення повноти) формалізованої бази шаблонів (правил, сигнатур) кібернетичних атак, як зворотна величина

від середньої тривалості $\overline{T}_{abs}$ періоду оновлення (від англ. *absolute* – повний, повнота). При цьому:

1. Часова затримка між моментом реєстрації характерних ознак відомої кібернетичної атаки, її автоматичним розпізнанням та блокуванням – нульова. Це цілком коректна, досяжна умова на сучасному етапі технічної реалізації промислових СВВ.

2. Часова затримка між початком та завершенням оновлення бази формалізованих шаблонів (правил, сигнатур) кібернетичних атак – нульова.

У практичному плані це досягається завдяки дотриманню концепції багатопотокового виконання при розробці процедур оновлення промислових СВВ, які вступають в силу миттєво, відразу після завершення прихованого ззовні паралельного з основною роботою завантаження змін.

Таким чином, ми завершили розгляд складових частин, показників виразу (1), а також порядку визначення величин показників у часі, виходячи з їх природи. Цільове призначення запропонованого підходу полягає у наданні адміністративному персоналу формального апарату для кількісної оцінки поточного стану кібернетичної безпеки $\Re(t)$ у будь-який момент τ на часовому інтервалі $\overline{T}_{abs}$ кроків функціонування АС асоційованого з тривалістю періоду оновлення формалізованої бази шаблонів (правил, сигнатур) кібернетичних атак. Слід відмітити відносну простоту, наочність моделі для програмної реалізації у формі відповідної автоматизованої функції діяльності адміністративного персоналу АС.

Суттєвою характерною рисою даного підходу є орієнтування на динаміку можливих змін $\Re(t)$ у ході функціонування АС для одержання поточної оцінки, що вигідно його відрізняє від низки підходів статичної природи, наприклад, від оцінки ризиків. У зв'язку з цим, величини показників w_{ij}, d_k^l, $P_{dm}^k\left(\overline{T}_{dm} \le T_{opt}\right)$ у складі виразів (2), (3), (6) відповідно мають сенс для визначення тільки у ході моделювання, натурного експерименту чи практичної, як результат роботи відповідних автоматизованих функцій у складі програмного забезпечення діяльності адміністративного персоналу АС.

Далі наводяться деякі результати (рис. 3) чисельного аналізу залежності (1) при певному наборі штучних варіантів динамічного тла на часовому інтервалі тривалістю $\overline{T}_{abs}$ перебування АС у l-му стані при граничному ідеалізованому припущенні $\overline{T}_{dm} \to \min$,

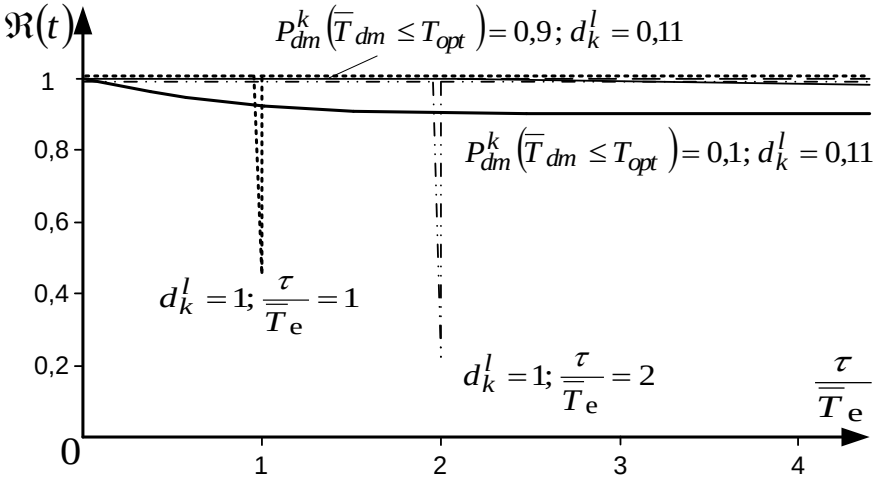

Рис. 3. Приклади залежностей $\Re(t)$

психофізичного обмеження, щодо максимально можливої кількості ситуацій придатних для одночасного аналізу однією адміністративною особою верхнього значення відомого ергономічного діапазону 7 ± 2 [20], а також за умови:

– $W_l = 1, P_{dm}^k\left(\overline{T}_{dm} \le T_{opt}\right) = 0{,}9,\ d_k^l = 0{,}11$ на всьому часовому інтервалі $\overline{T}_{abs}$;

– $W_l = 1, P_{dm}^k\left(\overline{T}_{dm} \le T_{opt}\right) = 0{,}1,\ d_k^l = 0{,}11$ на всьому часовому інтервалі $\overline{T}_{abs}$;

– $W_l = 1, P_{dm}^k\left(\overline{T}_{dm} \le T_{opt}\right) = 0{,}1,\ d_k^l = 1$ в момент часу $\tau \diagup \overline{T}_{abs} = 1$;

– $W_l = 1, P_{dm}^k\left(\overline{T}_{dm} \le T_{opt}\right) = 0{,}1,\ d_k^l = 1$ в момент часу $\tau \diagup \overline{T}_{abs} = 2$.

Висновки

На сучасному етапі практичного застосування методів теорії розпізнання образів для виявлення і блокування спроб реалізації загроз безпеки інформації АС кібернетичної природи основним дієвим способом залишається систематичне оновлення бази формалізованих шаблонів (правил, сигнатур) *IDS*, що стали відомі з часом, тобто забезпечення її повноти.

Вважається, що своєчасне виявлення і блокування всіх відомих кібернетичних атак дозволяє повністю уникнути потенційної шкоди внаслідок їх здійснення.

При цьому нові, невідомі *IDS* за характерними ознаками кібернетичні атаки у разі здійснення зі значною ймовірністю призводять до нанесення шкоди певної величини, а їх виявлення і блокування цілком покладається на адміністративний персонал АС.

Завдяки низки відомих психофізичних обмежень організація роботи оператора *IDS* з числа адміністративного персоналу АС лежить у науковій площині методів синтезу програмно-технічних систем підтримки прийняття рішень відповідного цільового призначення.

Запропонований показник кібернетичної безпеки АС є одним з ключових критеріїв відбору варіантів у ході вирішення наукової задачі синтезу системи кібернетичної безпеки АС.

ЛІТЕРАТУРА

1. Бірюков В.О., Єсаулов М.Ю., Жук П.В., Міночкін А.І., Павлов І.М. Теоретичні основи інформаційної боротьби в сучасних війнах, воєнних конфліктах та у війнах майбутнього/ – Підручник. – К.: ВІТІ ДУТ. – 2013. – 322 с.

2. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.

3. Хогланд, Грег, Мак-Гроу, Гари. Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом “Вильямс”, 2005. – 400 с.: ил.

4. Ховард М., Лебланк Д., Виега Д. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок . – М.: Издательский дом ДМК-пресс, 2006. – 288 с.: ил.

5. Воєнна політика, безпека і стратегічне планування. Інформаційна безпека держави у воєнній сфері. Терміни та визначення: Військовий стандарт ВСТ 001.004.004 – 2014 (1). – Київ: Міністерство оборони України, 2104. – 22 с.

6. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1– 003 – 99. – Київ: ДСТСЗІ СБ України, 1999. – 26 с.

7. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій: Навч. посібник. – К.: ДУІКТ, 2009 – 450 с.

8. Антонюк А.О., Жора В.В. Теоретичні основи моделювання та аналізу систем захисту інформації: [монографія] / А.О. Антонюк, В.В. Жора. – Ірпінь: Національний університет ДПС України, 2010. – 310 с.

9. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1 – 002 – 99. – Київ: ДСТСЗІ СБ України, 1999. – 16 с.

10. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2 – 004 – 99. – Київ: ДСТСЗІ СБ України, 1999. – 23 с.

11. Таненбаум Э. Современные операционные системы. 3-е изд. – СПб.: Питер, 2012. – 1120 с.: ил. – (Серия „Классика computer science”).

12. CommonVulnerability Enumeration // – Режим доступу: http://cve.mitre.org (9.03.15).

13. CommonWeakness Enumeration // – Режим доступу: http:// cwe.mitre.org (9.03.15).

14. Common Attack Pattern Enumeration and Classification // – Режим доступу: http://capec.mitre.org (9.03.15).

15. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений / Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. – М.: ДМК Пресс, 2004. – 616 с.: ил. – (Серия „Администрирование и защита”).

16. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – К.: ООО „ТИД” „ДС”, 2001. – 688 с.

17. Левин Б.Р. Теория надежности радиотехнических систем (математические основы). Учебное пособие для вузов. М., „Сов. радио”, 1978, 264 с.

18. Вероятностные методы в вычислительной технике: Учеб. пособие для вузов по спец. ЭВМ / А.В. Крайников, Б.А. Курдиков, А.Н. Лебедев и др., Под ред. А.Н. Лебедева и Е.А. Чернявского. – М.: Высш. шк., 1986. – 312 с.: ил.

19. Хусаінов П.В. Система інформаційної підтримки адміністратора безпеки: структура, задачі, оцінка ефективності // Збірник наукових праць ВІТІ НТУУ „КПІ”. – Випуск № 3. – К.: ВІТІ НТУУ „КПІ”, 2007. – С. 148 – 155.

20. Хусаінов П.В. Методика визначення раціональної послідовності надання інформаційних повідомлень оператору системи захисту// Збірник наукових праць ВІТІ НТУУ „КПІ”. – Випуск № 3. – К.: ВІТІ НТУУ „КПІ”, 2006. – С. 148 – 155.