По-друге, це забезпечення фізичної безпеки визначених матеріальних носіїв інформації комп'ютерних систем від підмін, порушення цілісності, для ідентифікації та автентифікації тощо шляхом їх радіоізотопного маркування.

По-третьє, це забезпечення безпеки фізичного стану здоров'я користувачів при роботі за комп'ютером.

Список літератури

1. А.Ю.Щеглов. Защита компьютерной информации от несанкционированного доступа. // Изд. Наука и Техника, С.Петербург, 2004г. – С.384.
2. Шорошев В.В. Модель угроз для локальних вычислительных сетей по рекомендаціям Конвенции Сонета Европы о кибеопреступности. Науково-виробничий журнал Державної адміністрації зв'язку та інформатизації України "Зв'язок" № 4, 2005. С. 37-42.
3. В.В.Шорошев, І.Л.Близнюк. Монографія "Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах органів внутрішніх справ України" (шифр "Торсіон-1"). Свідоцтво Державного департаменту інтелектуальної власності Міносвіти і науки України про реєстрацію авторського права на твір № 14446 від 20.11.2005 у вигляді робот изПого продукту "Торсіон-1". – К.: Видавництво НАВСУ, 2003р. – 316с.
4. І.І.Пающик. В.В. Шорошев. Захист носіїв інформації з використанням радіоізотопів // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Вид. НТУ «КПІ», випуск №5-2002. – С.77 – 83.
5. І.І.Пающик, В.В.Шорошев, Ю.І.Федоренко. Проблема захисту матеріальних носіїв інформації з використанням радіоізотопів. // Науковий вісник НАВСУ. – К., 2003. - № 5. С.215-224.
6. Патент США N 4765655 "Маркування предметів мистецтв в цілях їх охорони за допомогою радіоактивних ізотопів ". 1988.
7. Патент Франції N 2597245 "Методика і прилад упізнання цінних предметів".1986.
8. Нормы радиационной безопасности НРБ – 76/87. Основные санитарные правила ОСП – 72/87. М.: Энергоатомиздат, 1988. – 160с.
9. Норми радіаційної безпеки України (НРБУ- 97); Державні гігієнічні нормативи. – Київ: Відділ поліграфії Українського центру держсанепідемнагляду МОЗ України,1997.- 125с.
10. А.Р.Павленко. Компьютер TV и здоровье. Решене проблемы. Издание четвертое, переработанное и дополненное. Изд. «КВИТ», г.Николаев, 2003. С. 239.
11. ГОСТ 12.1.005-88. Общие санитарно-гигиенические требования к воздуху рабочей зоны.
12. Положення про медичний огляд працівників певних категорій (ДНАОД 0.03-4.03-94), затверджене наказом МОЗ України від 31.03-94 № 45.
13. Наказ № 1214 від 26.11.2002 МВС України про затвердження Типової інструкції з охорони праці для працюючих з персональними комп'ютерами.
14. ДНАОП 3.3.2.007-98. Державні санітарні правила і норми робіт із візуальними дисплейними терміналами електронно-обислювальних машин.

Надійшла 24.03.2008р.

УДК 681.3.

В.С.Чередниченко

МОДЕЛЬ ПОШИРЕННЯ ЗАСОБІВ ПРИХОВАНОГО ІНФОРМАЦІЙНОГО ВПЛИВУ

Впровадження в інформаційні системи засобів прихованого інформаційного впливу (ЗПІВ), під якими розуміються комп'ютерні «хробаки», програмні закладки, комп'ютерні

віруси, а також змішані засоби прихованого впливу, може привести до порушення ваги, кількості й направленості зв'язку між компонентами системи, у результаті чого може відбутися перепрограмування цих компонентів й/або їх знищення.

Тому розробка методів пошуку і визначення меж поширення цих засобів є актуальним завданням. Крім того, варто відзначити, що дана проблема потребує системного прошарування й поширення підходів до моделювання поширення ЗПІВ з позицій інформаційного впливу інформаційних систем, які самонавчаються з метою визначення меж цього поширення. Як відомо, самонавчання являє собою здатність системи виділяти у вхідних потоках інформації аналітичні залежності, що дозволяють розглядати вхідні дані як основне джерело інформації й тим самим прогнозувати розвиток процесу. Отже, самонавчання є важливим атрибутом існування інформаційної системи. Виділення аналітичних залежностей може відбуватися в нечітко визначеній обстановці, і, отже, вхідні дані можуть бути також визначені нечітко.

Накладемо наступні обмеження:

Система З (зловмисник) намагається змусити систему ОН (обсяг нападу) діяти в інтересах системи З. Для досягнення цієї мети система З повинна шляхом прихованого (латентного) цілеспрямованого інформаційного впливу спробувати налаштувати систему ОН таким чином, щоб вселити їй вигідну для нападаючої системи З систему цінностей і правил поведінки. Система З для досягнення своїх цілей використає ЗПІВ. Програмно-техніне середовище системи ОН, у яку система З намагається впровадити ЗПІВ, назвемо ПТС.

Ефективність прихованого цілеспрямованого інформаційного впливу системи З на систему ОН у загальному випадку може залежати від наступних факторів:

- досягнення (вдалої доставки) ЗПІВ до системи ОН;
- відповідності навчальної вибірки (ЗПІВ), яка приховано подається на вхід системи ОН, поточному стану цієї системи, щоб бути в неї вбудованою.
- здатність системи ОН виявляти й контролювати зародження й розвиток ЗПІВ у власній структурі, вчасно їх блокувати й знищувати.

Етапи актуалізації ЗПІВ у загальному вигляді можна представити в такий спосіб: впровадження в ПТС → дослідження середовища впровадження → активізація з можливістю репродукції → модифікація (руйнування) ПТС. Актуалізація ЗПІВ у середовищі ПТС – не що інше, як один з різновидів їхньої інформаційної взаємодії.

Інформаційна взаємодія ЗПІВ системи З і ПТС системи ОН будемо розглядати з позицій взаємодії двох інформаційних об'єктів, з огляду на, що будь-який об'єкт є об'єкт-система (тобто може складатися з безлічі підсистем), і будь-який об'єкт-система належить хоча б одній системі об'єктів даного роду (тобто володіє тими самими ознаками). Під інформаційним об'єктом будемо розуміти елемент програми, що містить фрагменти інформації, що циркулює в цій програмі. Залежно від мови програмування в якості інформаційних об'єктів можуть виступати змінні, масиви, записи таблиці, файли, фрагменти оперативної пам'яті й т.д.[1].

У реальності будь-який об'єкт-система з відносинами різних типів і видів зв'язку з іншими об'єктами-системами, і залежно від завдань дослідження його можна розглядати і як самостійний об'єкт-систему, і як підсистему іншого більш складного об'єкта-системи (системи об'єктів даного роду). Виходячи зі сказаного інформаційна взаємодія ЗПІВ і ПТС як об'єктів-систем можна розглядати як систему об'єктів даного роду з наступними параметрами: m – компоненти системи; R – відносини (зв'язку) між компонентами системи; Z – види композиції компонентів по відносинам R. Тріада m, R, Z характеризує внутрішній стан цієї системи й визначає родові ознаки системи об'єктів даного роду < ЗПІВ – ПТС >. Отже, інформаційний вплив двох систем є система.

Побудова такої системи може бути здійснена у відповідності до наступного алгоритму [2]:

1. Відбір на уневерсума {U} на єдиній підставі $A_i^{(0)}$ деякої сукупності «первинних» елементів $\left\{M_i^{(0)}\right\}$.

2. Накладення на «первинні» елементи певних відносин єдності $R_i^{(1)}$ й утворення, завдяки цьому по даному $Z_i^{(1)}$ безлічі об'єктів – систем (композицій) $\{M_i^{(1)}\}$.
3. Зміна композицій множини $\{M_i^{(1)}\}$ й висновок (відповідно до відносин $R_i^{(2)}$, $R_i^{(3)}$, …, …, $R_i^{(S)}$ і законам композицій $Z_i^{(2)}$, $Z_i^{(3)}$, …, $Z_i^{(S)}$) множин композицій $\{M_i^{(2)}\}$, $\{M_i^{(3)}\}$, …, $\{M_i^{(S)}\}$, при яких ці композиції виявляються побудованими із частини або всіх «первинних» елементів тієї ж множини $\{M_i^{(0)}\}$.
4. Виведення всіх можливих для даних A_i, R_i, Z_i об'єктів-систем множини M_i або системи об'єктів даного i-го роду: $S_i = \{M_i\} = \{M_i^{(0)}\}, \{M_i^{(2)}\}, \{M_i^{(3)}\}, \ldots \{M_i^{(S)}\}$.

Наведений алгоритм дозволяє побудувати систему < ЗПІВ – ПТС> як систему об'єктів даного роду. Уведемо наступні позначення:

$L(latent)$ – ЗПІ (засоби прихованого інфікування);

$D(data)$ – дані;

$C(commend)$ – команди;

$N(indefinite)$ – невизначені інформаційні об'єкти, які однозначно не можна віднести ні до даних, ні до команд.

З урахуванням цих позначень ПТС уявимо як об'єднання множини об'єктів-систем, що складаються з множини команд $C = \{C_i\}$, множини даних $D = \{d_i\}$ і множини інших (невизначених) $N = \{n_i\}$ об'єктів-систем, які неможливо однозначно віднести ні до команд, ні до даних.

Засоби прихованого інформаційного впливу можна розглядати з деякими функціями приналежності μ_i і як підсистему (первинний елемент) ПТС впровадження $\{L, \mu_i\}$, і як частину перерахованих об'єктів-систем $\{c_i, \mu_c\}$, $\{d_i, \mu_d\}$, $\{n_i, \mu_n\}$.

Отже, у загальному вигляді ЗПІВ можуть знаходити й у вигляді окремої множини як підсистема ПТС $\{L, \mu_l\}$, і в кожній з перерахованих множин команд $\{C_i, \mu_c\}$, даних $\{d_i, \mu_d\}$ й інших $\{n_i, \mu_n\}$ об'єктів-систем.

Отже, систему < ЗПІВ – ПТС> позначимо в такий спосіб: $S_i = \{(M_i, \mu_M)\} = \{(M_i^{(L)}, \mu_L), (M_i^{(C)}, \mu_C), (M_i^{(D)}, \mu_D), (M_i^{(N)}, \mu_N)\}$. Тут композиції побудовані з первинних елементів M_i виділених за ознаками $a \in A_i^{(0)}$, побудованих по нечітким відносинам $r \in \{(R_i, \mu_R)\}$ і нечітким законам композиції $z \in \{(Z_i, \mu_Z)\}$ з функціями приналежності $\mu_M(m)$, $\mu_R(r)$, $\mu_z(z)$.

Якщо припустити, що умова $\{M_C, \mu_C\} \cap \{M_D, \mu_D\} \neq Ш$ може виконуватися досить рідко, то з розгляду його можна виключити.

З урахуванням сказаного, об'єднання перерахованих вище множин утворить всю множину об'єктів-систем M у системі об'єктів даного роду, що в загальному випадку може бути виражене в такий спосіб: $M = \{M_i, \mu_i\} = \{M_L, \mu_L\} \cup \{M_C, \mu_C\} \cup \{M_D, \mu_D\} \cup \{M_N, \mu_N\}$.

Для виявлення межі системи < ЗПІВ – ПТС>, тобто межі поширення засобів прихованого інформаційного впливу системи З у ПТС системи ОН може бути застосований метод, звичайно використовуваний при дослідженні екосистем [3], суть якого полягає в тому, що будь-яка система об'єктивно є екосистемою і при дослідженні завжди розділяється на дві підсистеми: «центральна» система (ЦС), з погляду якої всі інші компоненти досліджуваної системи розглядаються як середовище й умови існування виділеної системи: «середовище», «ресурси».

ЦС – це виділений по деякій ознаці компонентів-системи, рівень активності якого залежить від сукупності ціннісних відносин, якісних і кількісних характеристик цього компонента й середовища, а його структурні зв'язки з іншими системами визначають взаємодія між ним і оточуючим його середовищем і встановлюють межі цієї системи.

Сказане можна записати в такий спосіб:

$$I_{П}^{ЦС} = f\left(I_{ф}, \left\{P_{rЦС}, P_{rсеред}, P_{ЦС-середовище}\right\}\right),$$

де $I_{П}$ – інтенсивність прояву (активності) ЦС;

$I_{ф}$ – інтенсивність сукупності зовнішніх, стосовно ЦС, факторів;

$P_{rЦС}$ – властивості ЦС;

$P_{rсеред}$ – властивості середовища;

$P_{ЦС-середовище}$ – сукупність відносин ЦС і середовища.

З урахуванням цього можна записати:

$\langle ЗПВ - ПТС\rangle \equiv EC \equiv \left\{\{ЦС\}, \{R_{ЦС-СР}\}, \{Z\}\right\}$, де <ЗПВ – ПТС> система «інформаційний вплив»;

ЕС – екосистема;

ЦС – центральна система, виділена в системі <ЗПВ – ПТС>;

$R_{ЦО-СР}$ – відношення <центральна система – середовище>;

Z – види композицій ЦС по відносинам R.

Виділення «центральної» системи як об'єкта-системи здійснюється по ознаці пов'язаності компонентів одним ступенем спільності, що дають підставу для присвоєння їм певної таксономічної категорії.

Як ознака, невикористовуваної для виділення ЦС при аналізі інформаційної взаємодії двох систем, може бути використана повнота семантичного збігу образів ЗПВ із фрагментами досліджуваного програмного масиву, обумовлена за допомогою функції приналежності μ_i. Тому завдання аналізу системи < ЗПВ – ПТС> може полягати в знаходженні ознак, властивих ЗПВ, що реалізують певні функції (наприклад, руйнуючі).

Ступінь подібності об'єктів-систем один на одного й близькості мови розпізнавання (взаєморозуміння) між ними в середовищі впровадження може характеризуватися функцією приналежності μ_i, визначаючи їхню приналежність до системи об'єктів даного роду. Функція приналежності характеризує сукупність ознак, що дозволяють відокремити впроваджений об'єкт від інших компонентів програмного забезпечення.

Фундаментальною характеристикою будь-якої системи, у тому числі системи < ЗПВ – ПТС>, є існування, що зводиться до трьох форм: просторової; тимчасової і динамічної.

Просторова форма існування системи < ЗПВ – ПТС> характеризується тим, що її межі поля екосистеми визначаються структурними зв'язками ЦС, виділеної в якості одиниці аналізу.

Тимчасова форма існування системи < ЗПВ – ПТС> характеризується тим, що взаємодія між різними системами здійснюється тільки при збігу інтервалів часу активності обох систем.

Динамічна форма існування системи < ЗПВ – ПТС> характеризується стабільністю й взаєморозумінням.

Мінливість припускає наявність у системи здатності до знищення й/або створенню її компонентів (нових об'єктів-систем) при надходженні в неї нової інформації. Стабільність припускає наявність у системи здатності до «самонавчання», яка характеризує зворотний зв'язок, що коректує поводження системи в її оточенні. Взаєморозуміння припускає прийнятність (розпізнавання) форми подання переданих повідомлень при інформаційному впливі систем (мова спілкування).

Можна припустити, що рівень взаєморозуміння як мовний аспект динамічної форми існування системи накладає обмеження на глибину структурних зв'язків між компонентами екосистеми, що встановлює межі екосистеми <ЗПВ–ПТС>.

Розглянемо розуміння елементом i елемента j_i для чого визначимо мову i-го елемента системи у вигляді множини пар так, як це пропонується в роботі [4]

$$S_i = \{(a_i, k, b_i, k)\}$$

де $0 \pi k \pi n_i$;

n – кількість можливих різних повідомлень у мові елемента i;

a_i, k – повідомлення, що надходить на вхід i-го елемента від елемента j_i;

b_i, k – повідомлення, що видається на виході i- го елемента у відповідь на повідомлення a_i, k;

$\mu(S)$– функція підрахунку кількості елементів множини.

Тоді рівень взаєморозуміння елементів i і j можна визначити в такий спосіб:

$$M_{i,j} = \frac{\mu(S_i \cap S_j)}{\max(\mu(S_i), \mu(S_j))},$$

а рівень розуміння елементом i елемента j буде визначатися:

$$m_{i,j} = \frac{\mu(S_i \cap S_j)}{\mu(S_i)}.$$

Звідси видно, що чим більше загальних понять у двох мовах (мові джерела й мові споживача цих повідомлень), тим носії цих мов краще розуміють один одного й тем менше рівень семантичного шуму буде при передачі повідомлень. Стосовно розпізнавання ЗПІВ це означає, що чим ближче одна до одної мови ЗПІВ і ПТС, тим складніше їх відрізнити одну від одної.

Засоби прихованого інформаційного впливу, розглянуті як об'єкти-системи, впроваджені в ПТС й, які утворили в результаті систему об'єктів даного роду, є частиною системи й, з одного боку, мають певну самостійність, а з іншого боку – взаємозалежні в межах цієї системи. При цьому характеристики k-го ЗПІВ з j-ой ПТС $I_j : (j = 1...m, j \neq k)$, вираження через функції приналежності μ_k, утворять взаєморозуміння k-го ЗПІВ з j-ой ПТС, якщо обробляючи j-го ПТС, можна одержати інформацію про k-м ЗПІВ. Інакше кажучи, чим вище значення функції приналежності $(0 \leq \mu_i \leq 1)$, тим більше ймовірність того, що в даній множині присутнє ЗПІВ.

Умова виникнення лавиноподібного процесу в результаті актуалізації ЗПІВ у середовищі ПТС може бути визначене з наступного вираження:

$$Y = K_t(1 - P_a)(1 - P_b)(1 - P_c),$$

де K – коефіцієнт репродукції ЗПІВ;

t – час життя ЗПІВ;

P_a – імовірність виявлення й ліквідації ЗПІВ захисними механізмами ПТС;

P_b – імовірність зворотного переродження ЗПІВ у нормальну програму;

P_c – імовірність спрацьовування механізму самоліквідації ЗПІВ.

З наведеного вираження виходить, що процес набуває лавиноподібний характер, якщо $Y \phi 1$. При цьому, чим більше Y перевищує 1, тим вище швидкість наростання лавиноподібного процесу.

Динаміку настання в розвитку загрозливих подій для системи ОН можна проаналізувати за допомогою фазової діаграми розвитку інформаційної взаємодії, що докладно дослідженно в роботі [5]. Як було відзначено там, система піддавалася інформаційному впливу, з необхідністю нападу в крапку біфуркації. Перебуваючи на околицях цієї крапки система може або перейти в стерпні умови існування й загинути, або змінити свою структуру, перейти в стерпні умови, а потім – в оптимальні для свого існування умови. Отже, крапка біфуркації

характеризується структурною кризою, адекватною формою рішення якої є структурна перебудова системи.

Час перебудови інформаційної системи $t_{пер}$ характеризується особливостями її структури, стабільність якої до різних впливів характеризується кількістю, спрямованістю й вагою зв'язків між її компонентами.

Визначення часу, наявного в інформаційної системи на структурну перебудову, здійснюється шляхом прогнозування можливого підвищення системи. Метод прогнозування полягає в тому, щоб оцінити, чи встигає система відреагувати на множину зовнішніх впливів за час t, характерна для даної структури, чи ні. Якщо не встигає, то необхідно змінити свою структуру, якщо в ній бракує елементів зв'язків, необхідних для такого блокування.

Викладене дозволить сформулювати істотні, необхідні й стійкі (повторювані) відносини, що виникають у процесі інформаційного впливу інформаційних систем.

Інформаційна система може перебувати в стані оптимального функціонування тільки протягом обмеженого часу t. Цей стан характеризується блокуванням усіх каналів інформаційного впливу й через час $t + \Delta t$ у чинність свого існування перейде в стан, при якому виникають нові канали. Зворотний перехід можливий тільки в результаті структурної перебудови системи.

Впровадження ЗПІВ у ПТС інформаційної системи є одним з видів взаємодії інформаційних систем.

Інформаційна взаємодія інформаційних систем являє собою систему, межі якої визначаються глибиною структурних зв'язків між її компонентами, які характеризуються мовними аспектами динамічної форми існування системи.

Список літератури

1. Коженеський С.Р., Кузнєцов Г.В., Хорошко В.О., Чирков Д.В. - Термінологічний довідник з питань технічного захисту інформації/ За ред. проф. В.О. Хорошка, вид.4-е, доповнене й перероб. - К.: Вид. ДУІКТ, 2007.-365с.
2. Браіловський М.М., Головань С.М. та інші. – Технічний захист інформації на об'єктах інформаційної діяльності/ За ред.проф. В.О. Хорошка. – К.: Вид. ДУІКТ, 2007. – 178с.
3. Расторгуев С.П. Инфицирование как способ защиты жизни. Вирусы: биологические, социальные, психические, компьютерные. – М.: Яхтсмен, 1996. – 121с.
4. Азаров С.С., Хорошко В.А. – Современные методы провайдинга. – К.: ПолиграфКонсалтинг, 2006. - 98с.
5. Волобуев С.В. к вопросу об информационном взаимодействии систем // Вопросы защиты информации, № 4, 2002. – с.2-7.

Надійшла 18.03.2008р.

УДК 65.012.8/342.738(477)

С.Л.Емельянов

НЕКОТОРЫЕ ВИДЫ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ОРУЖИЯ

Постановка проблемы. Согласно прогнозам XXI столетие станет веком глобальной информатизации и компьютеризации всего мира и переходом человечества к новому информационному обществу, в котором решающая роль отводится информации,