10. До проблеми організації захисту інформації на підприємствах / Г.Б. Жиров, В.Б. Бахвалов, Н.М. Берназ, Є.С. Лєнков // Інформаційна безпека: наук.-практ. конф., Київ, 26-27 бер. 2009 р.: тези доп. – К.: ДУІКТ, 2009. – С. 67–71.

11. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28 квітня 1999 року № 22.

У статті розглянута загальна математична модель об'єктів захисту інформаційно-телекомунікаційної системи оперативного інформування МВС України, яку необхідно враховувати при подальшому удосконаленні побудови ефективної комплексної системи її захисту від порушників безпеки.

В статье рассмотрена общая математическая модель объектов защиты информационно-телекоммуникационной системы оперативного информирования МВД Украины, которую необходимо учитывать при дальнейшем усовершенствовании построения эффективной комплексной системы ее защиты от нарушителей безопасности.

Рецензент:д.т.н., проф.Хорошко В.О.
Надійшла 12.10.2010

УДК 004.621 **Берназ Н.М.**

МОДЕЛЮВАННЯ ПРОТОКОЛІВ ВЗАЄМОДІЇ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ

Системи захисту інформації, що орієнтовані на масове використання у різних прикладних системах, повинні бути мобільними, тобто достатньо легко повинні переноситися з одного середовища на інше, яке підлягає захисту. У зв'язку з цим, є актуальною задача проникнення (занурення) системи захисту в захищуване середовище. Для розв'язання цієї задачі необхідно дослідити інтерфейси взаємодії мобільної системи з користувачем та системою, що підлягає захисту, а також процедури адаптації системи захисту до захищуваного середовища. Крім цього, важливим є визначення параметрів адаптації, основними серед яких можна назвати характеристики і критерії, що задають рівень безпеки об'єкта захисту.

Мобільні системи захисту, на відміну від мобільних операційних систем, повинні вирішувати цілий ряд специфічних задач на етапі їх встановлення в захищувану систему. До таких задач слід віднести наступні задачі:

- визначення інформаційно небезпечних компонент в захищуваній системі;
- визначення необхідного рівня захисту для окремих компонент і системи в цілому;
- встановлення програмного взаємозв'язку між системою захисту та захищуваним середовищем;
- адаптацію інтерфейсу користувача захищуваної системи до вимог мобільної системи захисту;
- формування інтерфейсу системи захисту в рамках функціональних задач захищу ваної системи.

Коротко зупинимося на загальному аналізі приведених задач, які необхідно розв'язувати.

Визначення інформаційно небезпечних компонент захищуваної системи є необхідною умовою впровадження і використання систем захисту. Ця задача принципово відрізняється від відомих задач, які розв'язуються в рамках існуючих систем контролю або перевірки систем захисту. В рамках останнього засобу розглядаються наступні ознаки можливих атак:

відмова в обслуговуванні; спроба несанкціонованого доступу; підготовка до атаки; підозріла активність; підозрілі команди на рівні протоколів.

Особливість задач виявлення інформаційно небезпечних елементів в прикладній системі полягає у наступному:

- відбувається виявлення і встановлення інформаційно небезпечних елементів прикладної системи на відміну від виявлення можливого проникнення упередженого втручання через систему захисту;
- предметна область інтерпретації прикладної задачі є однією з вихідних передумов для визначення інформаційно небезпечних елементів;
- на початковій стадії використання мобільної системи захисту реалізується декларативний принцип захисту.

Використання будь-яких додаткових засобів, в тому числі, засобів захисту, вимагає обгрунтування, яке в даному випадку представляє собою систему вимог до забезпечення відповідного рівня захисту. Ці вимоги з одного боку можуть пов'язуватись з відомими класифікаціями рівнів захищеності [1]. З другого боку, рівень захищеності повинен бути узгоджений в першу чергу з тими вимогами, які формуються на основі оцінки можливих реальних втрат, які можуть бути заподіяні, при порушенні безпеки інформаційних компонент, або на основі суб'єктивних позицій власника засобів реалізації прикладної системи. Оскільки засоби, що реалізують те чи інше інформаційне середовище можуть бути приватними, як і саме інформаційне середовище, то така позиція в визначенні рівня захисту інформації має право на існування. Таким чином, однією з важливих ознак мобільних систем захисту є їх здатність достатньо гнучко визначати можливість забезпечення того чи іншого рівня захисту, виходячи з наперед встановлених принципів його визначення.

Встановлення програмних взаємозв'язків між засобами розв'язання прикладної задачі та компонентами засобів захисту інформації може справляти враження чисто технічної задачі. Для мобільних систем захисту, розв'язання цієї задачі є принциповим, оскільки її мобільність зобов'язує систему захисту максимально автоматизувати цей процес. В рамках мобільних систем ця задача розв'язується шляхом створення відповідних універсальних внутрішніх інтерфейсів, які функціонально універсальні і дозволяють на рівні управління процесами, або на рівні управління задачами взаємодіяти з прикладною системою. Особливість мобільної системи захисту в рамках цього аспекту полягає ще й в тому, що система захисту повинна адаптуватись до прикладних задач, що розв'язуються в захищуваній системі. Це обумовлено тим, що алгоритми розв'язку прикладних задач можуть мати в різних прикладних системах власну специфіку реалізації однотипних задач.

Існує широкий спектр прикладних систем, що потребують захисту. Таким чином, відповідні системи мають розвинені інтерфейси зв'язку з користувачами. При використанні системи захисту не доцільно з огляду на задачі захисту переробляти ці інтерфейси, тим більше, що мобільна система захисту може встановлюватися в прикладну систему на етапі експлуатації останньої. Отже, мобільна система захисту повинна дозволяти адаптацію прикладних інтерфейсів до власних потреб, забезпечуючи при цьому максимальне сприяння взаємозв'язку користувача з системою. Досить часто це може досягатись методом формування прозорих для користувача інтерфейсів підтримки компонент захисту.

Не викликає сумнівів, що захищувана система, або прикладна система, мусить взаємодіяти з засобами захисту не тільки на рівні взаємозв'язків прикладної системи з користувачем, але й на рівні взаємодії з процесами, що відбуваються в прикладній системі. Це обумовлено в першу чергу тим, що джерелами загроз можуть виявитися упереджені втручання в роботу системи, які не використовують інтерфейси користувачів системи. Наприклад, такі втручання можуть здійснюватись через системні термінали, або шляхом впровадження програм агентів через мережеві засоби зв'язку прикладної системи з зовнішнім інформаційним середовищем. Можливі методи розв'язку цих задач можуть полягати в

створенні інтерфейсів орієнтованих на взаємодію системи захисту з прикладною системою. Такі інтерфейси являються спеціалізованими і представляють собою прототип відомих інтерфейсів, що використовуються в апаратурних засобах для конфігурування основних апаратних компонент в обчислювальній техніці.

Очевидно, що побудувати достатньо універсальний інтерфейс, який задовольняв би всім вимогам, що можуть висуватися довільними прикладними системами, досить важко. Тому в рамках мобільної системи захисту повинна існувати деяка система, що може моделювати достатньо широкий по своїх можливостях спектр інтерфейсів з різними можливостями чи параметрами, які задовольняли би вимогам прикладних систем, у які впроваджуються системи захисту, а також всім вимогам, яким необхідно, в кожному конкретному випадку, задовольняти, щоб система захисту могла забезпечити потрібний рівень захисту прикладної системи.

У відповідності з теорією моделювання [2] засоби моделювання повинні представляти собою формалізований опис процесів, які моделюються. Цей опис повинен представляти собою інваріант реальних процесів, які необхідно моделювати. Розглянемо деякі підходи до створення таких моделей. Розглянемо уявлення про взаємозалежні логічні функції. Ці взаємозалежності будемо визначати виводимістю однієї функції з іншої. Таким чином, система взаємозалежних функцій може представляти собою множину висловлювань, якими описується інтерфейс. Відомо, що інтерфейси і відповідні протоколи їх реалізації описують взаємодію як мінімум двох сторін. Тому в якості моделі, що описує відповідну множину можливих протоколів, можна використовувати систему висловлювань. Нехай S представляє собою таку систему, Q1 і Q2- дві незаперечні множини висловлювань, що включають S і $Q_1 \cap Q_2 \supset S$. Якщо $C(Q_1) \cap C(Q_2) \subset C(S)$, де C - алфавіт, в якому будуються системи висловлювань, то $Q_1 \cup Q_2$ незаперечні. Необхідність встановлення умов незаперечності деякої множини висловлювань є гарантією незаперечності механізмів реалізації кожного окремого інтерфейсу, якщо вони задовольняють встановленим вимогам. Розглянемо незаперечність об'єднання двох окремих незаперечних множин висловлювань в рамках вищевикладених умов. Якщо $Q_1 \cup Q_2$ незаперечні, то можна знайти такі скінчені $\{X_1,...,X_n\} \subset Q_1$, $\{Y_1,...,Y_k\} \subset Q_2$, що $X \& Y$ заперечне, де $X=X_1 \& ... \& X_n$ і $Y=Y_1 \& ... \& Y_k$, при $n \geq 1$, $k \geq 1$. При цьому $\{X\} \cup S$ і $\{Y\} \cup S$ незаперечні, оскільки $Q_1 | S \cup \{X\}$, а $Q_2 | S \cup \{Y\}$. Тому можна перейти до доведення умови, що $X_1 \& X_2$ незаперечне, якщо X1 сумісне з S і X2 сумісне з S і два висловлювання X1 і X2 такі, що має місце $C(X_1) \cap C(X_2) \subset C(S)$, де S - повна множина висловлювань. Нехай $X_1 = Y_1(a_1,...,a_m)$ і $X_2 = Y_2(b_1,...,b_n)$, де явно виписані ті індивіди, яких немає в S. Приймемо, $Z_1 = [\exists x_1,...,\exists x_m Y_1(x_1,...,x_m)]$ і $Z_2 = [\exists y_1,...,\exists y_n Y_2(y_1,...,y_n)]$. Кожне Z_1 і Z_2 окремо сумісні з S, а тому по допущенню $Z_1 \& Z_2$ незаперечне. Якщо ж $X_1 \& X_2 = Y_1(a_1,...,a_m) \& Y_2(b_1,...,b_n)$ заперечне, то висловлювання:

$$Z = \exists x_1,...,\exists x_m \exists y_1 ... y_n [Y_1(x_1,...,x_m) \& Y_2(y_1,...,y_n)]$$

також повинно бути заперечним. Але $|Z = Z_1 \& Z_2$, а $Z_1 \& Z_2$ як показано вище незаперечне. Тому можна припустити, що:

$$C(X_1) \subset C(S), \; C(X_2) \subset C(S).$$

Нехай D1- модель $S \cup \{X_1\}$, D_1^* - структура, що отримана з D1 виключенням співвідношень, що не входять в S. Позначимо через S_1^* множину всіх висловлювань, визначених і істинних в D_1^*. Оскільки X_2 сумісне з S, а D_1^* - модель S, то множина $S_1^* \cup \{X_2\}$ незаперечна. Нехай D2 - модель цієї множини і D_2^* - структура одержана з D2 виключенням співвідношень, що не входять у S. D_2^* - будучи моделлю S_1^*, являється елементарним розширенням D_1^*. Звідси витікає існування елементарного розширення D3 структури D1, яке також є елементарним розширенням D_2^*, якщо ігнорувати співвідношення, що не входять в D_2^*. Таким чином, знову D_3^* є структура, яка є елементарним розширенням D3, таким, що D_2^* є елементарне розширення D2, де D_3^* одержано з D2 виключенням співвідношень, які не входять в D_2^*. Продовжуючи цю побудову, можна отримати послідовність структур $D_1, D_2, D_3, ..., D_n, ...$ і відповідні послідовності $D_1^*, D_2^*, D_3^*, ..., D_n^*, ...$, причому будуть виконуватись наступні умови. Структури $D_1, D_3, D_5, ...$ будуть мати одинакові співвідношення і $D_1 rr D_3 rr D_5 rr ...$. Аналогічно, структури $D_2, D_4, D_6, ...$ мають одні і ті ж співвідношення і має місце $D_2 rr D_4 rr D_6 rr ...$. На кінець, $D_1^* rrr D_2^* rrr D_3^* rrr ...$ причому D_1^* отримується з D_i, якщо обмежитися тільки співвідношеннями S, що належать структурам з парними і непарними індексами.

Нехай має місце співвідношення:

$$D^* = \bigcup_n \{D_n^*\}, \quad D' = \bigcup_k \{D_{2k+1}\} \quad \text{і} \quad D'' = \bigcup_k \{D_{2k}\}.$$

Множини індивідів трьох структур D^*, D', D'' співпадають, і крім того, D^* можна отримати з D' і D'' викидаючи співвідношення, що не містяться в S. Визначимо структуру D приєднуючи до D^* співвідношення D' і D''. Оскільки спільними співвідношеннями являються співвідношення D^*, то прийняте визначення коректне. Однак D1 задовольняє X1, а тому D_3, D_5 і, на кінець, D' задовільняють X. Аналогічно, D задовільняє X і відповідно, $D_4, D_6, ...$ і, на кінець, D'' задовольняє X2, а тим самим і кон'юнкції $X_1 \& X_2$.

Інтерфейси двох систем представляють собою дві взаємодіючі структури і тому необхідно більш конструктивно розглянути можливу взаємодію. Розглянемо інтерфейси як дві взаємозв'язані системи висловлювань Q і D.

Взаємозв'язаність означає наступне. Дві системи Q і D взаємозв'язані, якщо має місце наступне співвідношення:

$$[(Q \Rightarrow q_i) \& (q_i, D \Rightarrow d_i)] \vee [(D \Rightarrow d_i) \& (d_i, Q \Rightarrow q_i)].$$

З взаємозв'язаної взаємодії двох систем Q і D випливає існування ініціативи у однієї чи іншої системи. Під ініціативою системи Q або системи D будемо розуміти деяку формулу $\Phi(Q, D)$, яку будемо називати описом цілі активізації відповідних інтерфейсів. Під інтерфейсом взаємодії двох систем J будемо розуміти деяку послідовність висловлювань, або формул, яка представляє собою вивід формули цілі $\Phi(Q, D)$. Таким чином, ціль активізації

інтерфейсу між двома системами Q і D представляє собою формулу, вивід якої здійснюється з врахуванням обмежень на процедуру' побудови виводу, які можуть бути сформульовані наступним чином і описуватись відповідними умовами формально:

- процедура P виводу цілі $\Phi(Q,D)$ повинна використовувати систему або систему Q або систему D окремо, $[P(Q) \vee P(D)] \& IP(Q,D)$;
- процедура P повинна складатися з окремих етапів виводу і на кожному етапі виводу можлива наступна схема формування виводу $(Q, d_{i-1} \Rightarrow q_i) \vee (D, q_{i-1} \Rightarrow d_i)$;
- вивід цілі $\Phi(Q,D)$ повинен допускати опис процедури P у вигляді наступної послідовності: $d_1^i, q_1^j, d_2^i, q_2^j, ..., d_n^i, q_n^j \Rightarrow \Phi(Q,D)$.

Порядок використання системи висловлювань Q або D в процесі реалізації процедури виводу обумовлюється обмеженнями на способи реалізації діалогу між сторонами, що реалізують відповідний інтерфейс. Одна з умов реалізації інтерфейсу полягає в виконанні вимог виводимості формул q_i і d_i з Q і D відповідно. При виводі поточних q_i і d_i ініціативною формулою для формування процедур виводу рі з P будуть відповідно d_{i-1} або q_{i-1}, оскільки інтерактивний режим передбачає чергування відповідних формул. Приведемо визначення взаємооднозначності між d_{i-1} і q_i, або q_{i-1} і d_i.

Визначення 1. Взаємооднозначність між логічними формулами a і b, що позначається $a \leftrightarrow b$, означає, що по формулі a, при відповідному її розширенні, можна побудувати формулу b.

Розглянемо умови виводимості q_i або d_i або D відповідно, які регламентуються наступним твердженням.

Твердження 1. Поточне q_i або d_i виводиме з Q або D якщо q_{i-1} або d_{i-1} не призводить до протиріччя з Q або з D і допускає коректне розширення останніх.

Будемо розглядати випадок виводимості q_i з Q при ініціативній формулі d_{i-1}, оскільки випадок виводимості d_i з D при ініціативній формулі q_{i-1} може бути розглянутий аналогічно. Припустимо, що d_{i-1} приводить до протиріччя в системі Q. Це означає, що $c = d_{i-1} \cup Q \Rightarrow c | q' \& \neg q'$. Для діалогових систем характерний взаємодоповнюючий зв'язок між формулами d_{i-1} і q_i. Це означає, що q_i по відношенню до d_i може представляти собою розвиток d_{i-1}. Під розвитком d_{i-1} розуміється розширення q_{i-1} для d_i, яке не допускає двозначності. Це означає, що має місце $(d_{i-1} | q_i) \& \neg (d_{i-1} | q_i')$. Припустимо, що має місце співвідношення $d_{i-1} | \neg q_i$, тоді згідно з визначенням взаємооднозначності між d_{i-1} і q_i витікає, що має місце $\neg (d_{i-1} | q_i)$, або можна записати, що $d_{i-1} | q_i$. Нехай для формування послідовності $p_i(d_{i-1} | q_i)$ відповідна формула d_{i-1} в системі висловлювань Q не може забезпечити необхідного розширення. В цьому випадку можливі дві ситуації:

- система Q не є повною з точки зору реалізації і інтерпретації інтерфейсу;
- d_i приводить до протиріччя $c = d_{i-1} \cup Q$.

В першому випадку невідповідність Q і D інтерфейсу J може бути усунена шляхом розширення Q або D таким чином, щоб відповідність між J і $Q \cup D$ була встановлена. В

другому випадку, розглянемо наступну послідовність. Нехай $d_{i-1} \cup Q$ заперечна система. Це означає, що d_{i-1} і q_{i-1} не задовільняють умові взаємозалежності, тобто $\neg(q_{i-1} \leftrightarrow d_{i-1})$. Це в свою чергу означає, що q_{i-1} приводить до протиріччя в $c' = q_{i-1} \cup D$. Проводячи аналогічні міркування по відношенню до d_{i-k} і q_{i-k}, в силу скінченості реалізації p_i інтерфейса J, можна прийти до формули $\varphi(Q)$, яка є цільовою функцією реалізації інтерфейсу J. Але якщо $\varphi(C)$, де $C = (Q \cup D)$ призводить до протиріччя в C, то $\varphi(C)$ вибрана не коректно, що не допустимо при формуванні $\varphi(C)$. Таким чином другий випадок також не може мати місце. Отже формування і реалізація довільного $p_i(d_{i-1}, q_i)$ або $p_j(q_{i-1}, d_i)$ може бути здійснена за рахунок розширень Q і D.

Висновок

Для реалізації інтерфейсу J використовувались Q і D для реалізації P, то реалізація інтерфейсу J також допустима, якщо функція $\varphi(C)$ незаперечна з C.

Література

1. Information Technology Security Evaluation Criteria. Harmonized Criteria of France-Germany-Netherlands-United Kingdom. Department of Trade and Industry. – London. -2001.
2. Кейсрер Г. – Теория моделей / Кейсрер Г., Чэн Ч.Ч. –М.: Мир, 1977. -607 с.

В роботі розглядається моделювання протоколів взаємодії в системах захисту інформації. Визначені параметри адаптації, основними з яких є характеристики і критерії, що задають рівень безпеки об'єкта захисту. Надані підходи щодо побудови універсального інтерфейсу, який задовольняє всім вимогам, що висуваються прикладними системами.

Рецензент:д.т.н., проф. Лєнков С.В.
Надійшла 16.11.2010

УДК 004.056, 004.075 **Дудикевич В.Б., Гарасим Ю.Р.** (НУ «Львівська політехніка»)

МАТЕМАТИЧНА МОДЕЛЬ ОЦІНКИ ЖИВУЧОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ЗА СТАНОМ СИСТЕМИ

Вступ

В сучасних умовах широкої інформатизації суспільства, масового поширення засобів комп'ютерної техніки (які, в свою чергу, з'єднують в локальні, районні, корпоративні, глобальні мережі зв'язку), зростанню злочинних посягань та несанкціонованих дій над інформацією, необхідністю захисту як державної, військової інформації, так і промислової, комерційної, фінансової таємниць проблема захисту інформації стає все більш актуальною.

Системи захисту інформації (СЗІ), які є основним механізмом забезпечення безпеки корпоративних мереж зв'язку (КМЗ) повинні мати властивість живучості [1] для того, щоб функціонувати в «агресивному» середовищі при дії зовнішніх та внутрішніх дестабілізуючих факторів (ДФ). Ця необхідність зумовлена тим, що припинення функціонування СЗІ КМЗ внаслідок дії ДФ призводить до великих економічних, фізичних, інформаційних втрат або катастрофічних наслідків внаслідок реалізації загроз конфіденційності, доступності та цілісності інформації, яка в них функціонує.