VII Выводы

Проанализированы особенности реализации мобильных операционных систем на примере наиболее распространенной системы Palm OS с точки зрения их безопасности. Определены возможные угрозы, способы внедрения, распространения и исполнения вредоносного кода, а также приведены рекомендации по защите от этих угроз.

Рассмотренные методы моделирования динамических систем и соответствующие выражения (4–8) могут применяться для формального анализа поведения подсистемы защиты во времени и оценки ее реакции на угрозы вредоносного кода с учетом особенностей упрощенной реализации механизмов безопасности в карманных персональных компьютерах.

Литература: 1. IDC, "Market Mayhem: The Smart Handheld Devices Market Forecast and Analysis, 1999–2004", Report 22430, June 2000. 2. Kingpin and Mudge. Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats. @stake, Inc. 3. Palm, Inc., Palm OS Programmer's Companion, DN 3004–003. 4. McAfee.com, "Increased Protection for Wireless Users in Wake of Recent PDA Trojan Discovery", Press Release, September 5, 2001.

УДК 654.924

АЛГОРИТМ ФУНКЦИОНИРОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ СИСТЕМЫ БЕЗОПАСНОСТИ

Владимир Волхонский

Санкт-Петербургский Государственный университет аэрокосмического приборостроения

Аннотация: **На основе анализа обобщенной структурной схемы системы безопасности и ее основных элементов рассматривается последовательность принятия решений об обнаружении угроз составными частями системы. Предлагается математическая модель системы.**

Summary: **Based on general security system block diagram and its main element analysis of the sequence of decision about treats are accomplishing. Mathematical model of security system is offered.**

Ключевые слова: **Система безопасности, обнаружение угроз, модель, решение.**

Алгоритм функционирования системы охранно-пожарной сигнализации (ОПС), рассмотренный в [1], определяет логику работы ее основы – контрольной панели (КП) – в зависимости от состояния ее элементов и текущего режима работы. В то же время в ряде случаев необходимо выполнить анализ в более общем случае системы безопасности (СБ) и, как частный случай, системы ОПС с учетом анализируемых характеристик и параметров объекта для обнаружения угроз, алгоритмов их преобразования и принятия решений.

Развитие технологии и совершенствование алгоритмов обработки, повышение информативности элементов систем, с одной стороны, и усложнение функций систем безопасности, с другой стороны, привело к развитию такого нового направления, как многоуровневые системы принятия решений. С этой точки зрения можно выделить два основных типа СБ. Одноуровневые, когда решение об обнаружении требуемого события или угроз (нападение, возгорание и др.) и реакции системы на него принимается на одном уровне системы (в одном устройстве). Пример – автономный пожарный извещатель. После принятия решения о возгорании следует акустический сигнал тревоги. Многоуровневые системы, в которых решения об обнаружении угроз принимаются на различных уровнях системы. Например, срабатывание извещателя в системе охранной сигнализации (первичное решение о тревоге) не означает возникновения состояния тревоги. Это будет зависеть от ряда факторов (режим охраны или нет, используется ли алгоритм двойного срабатывания и т. п.), что определяется алгоритмом работы КП. Кроме того, даже при формировании сигнала тревоги панелью, окончательное решение может принимать центральная станция мониторинга.

Таким образом, с точки зрения принятия решений в составе некоторой системы охраны (централизованной, автономной, интегрированной и т. п.) имеют несколько уровней принятия решений о том или ином событии. Подобные системы, в которых как решения о регистрации тех или иных событий, так и решения о реакции элементов системы на эти события принимаются на различных уровнях будем называть системами с распределенными уровнями принятия решений или с распределенным «интеллектом».

I Обобщенная структурная схема СБ

В общем случае СБ должна обнаруживать угрозы охраняемому объекту, принимать решение об адекватном реагировании на угрозы и противодействовать им. То есть в составе системы безопасности в общем случае должны быть следующие элементы.

- Устройства обнаружения угроз (УОУ) охраняемому объекту или, в терминологии принятой в системах ОПС, извещатели.
- Системы сбора и обработки информации (ССОИ).
- Система противодействия и ликвидации угроз (СПЛУ).

Это позволит обобщить результаты на системы безопасности различного назначения (ОПС, контроля и управления доступом (КУД), защиты информации и др.), а также различного уровня интеграции [2] (комплексные, интегрированные, объединенные).

На рис.1 приведена обобщенная структурная схема такой системы, на основе которой сформулируем математическую модель СБ.

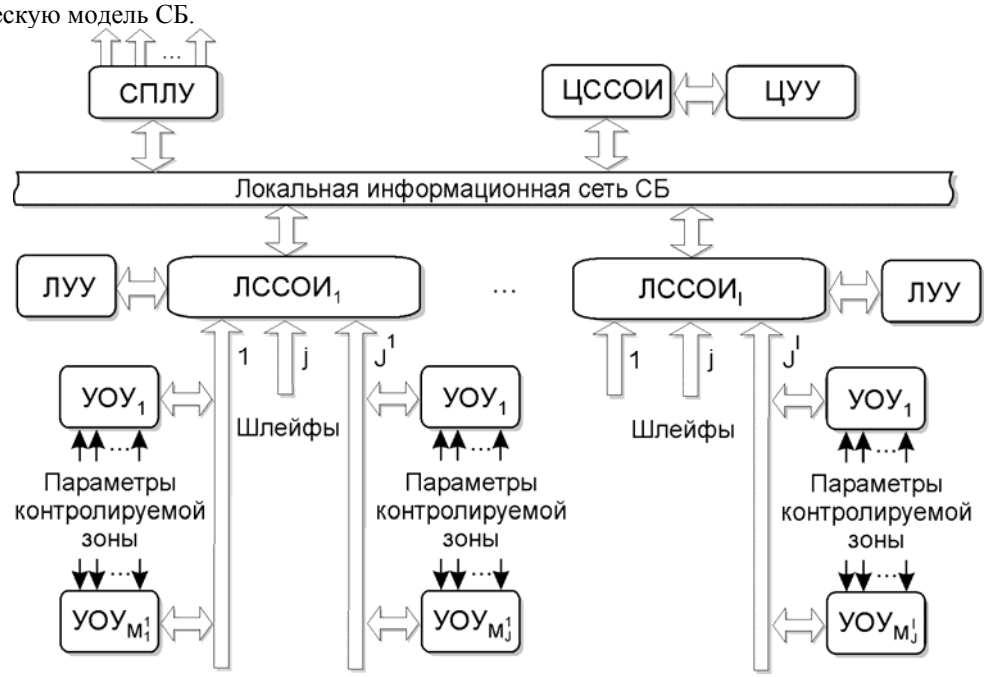

Рисунок. 1 – Обобщенная структурная схема СБ

СБ состоит из ряда подсистем. Первичный анализ состояния объекта, а точнее состояния контролируемой зоны охраняемого объекта, выполняют УОУ (извещатели) на основе анализа контролируемых физических характеристик и параметров этой зоны и заложенного в них алгоритма обработки. После принятия решения об обнаружении угроз контролируемому объекту (к примеру, таких как несанкционированное проникновение, нападение, возгорание, утечка информации, повышение концентрации газа и т. д.) извещатель изменяет соответствующим образом параметр шлейфа, в который он включен.

На следующем уровне локальная ССОИ (в таких типичных системах безопасности, как ОПС – это контрольная панель [1, 2] или приемно-контрольный прибор, в системах КУД – контроллер) выполняет анализ состояния шлейфов. В зависимости от схемотехнической реализации последнего, состояния УОУ и программной конфигурации ССОИ используется то или иное количество информативных признаков, на основе которых в соответствии с заданным алгоритмом и принимается решение о нарушении шлейфа (проникновение, неисправность, вскрытие, …).

На уровне локальной системы сбора и обработки информации о состоянии шлейфов и устройств управления принимается решение о состоянии ЛССОИ (или подсистемы). При этом, естественно, учитывается также ряд других важных параметров, в первую очередь состояние ЛССОИ – охрана (полная или частичная), снятие с охраны, тестирование,…. Информация о состоянии ЛССОИ передается через локальную информационную сеть СБ на центральную ССОИ (например, на пункт централизованной охраны или АРМ интегрированной системы безопасности).

На этом уровне (высшем приоритете) принимается окончательное решение о наличии угрозы и мерах реагирования – противодействию и ликвидации этой угрозы. Это может быть выполнено автоматически или

при участии оператора(ов) в соответствии с тактикой работы пункта охраны с помощью системы противодействия и ликвидации угроз (СПЛУ).

Таким образом, устройства, входящие в состав системы безопасности и реализующие алгоритм принятия решений (обладающие “интеллектом”), распределены дискретно как пространственно, так и структурно.

С точки зрения теории систем угрозы, проявляющиеся в определенных изменениях физических параметров среды (объекта), являются входными воздействиями на СБ. Реакция системы на эти угрозы (оповещение, противодействие, ликвидация,…) – выходными сигналами, а на режим работы – начальными условиями.

Итак, рассмотрим систему безопасности, включающую такие основные элементы, как устройства обнаружения угроз охраняемому объекту или извещатели, системы сбора и обработки информации (ССОИ), то есть контрольные панели, и СПЛУ.

В общем случае, имеем следующие элементы системы.

- Группу из локальных ССОИ (контрольных панелей или контроллеров); это могут быть как физические контрольные панели, так и логические, то есть программно формируемые разделы [1].

- J^i шлейфов у каждой i-й панели.

- M^i_j извещателей в j-м шлейфе i-й панели, при максимальном количестве извещателей в шлейфе $M^i = \max\limits_{j=1,J}(M^i_j)$.

N^i_{mj} контролируемых параметров $u^i_{jmn}(t)$ объекта в m-м извещателе в j-м шлейфе i-й панели.

II Анализ СБ

Информационные характеристики (признаки) или параметры контролируемого объекта $u^i_{jmn}(t)$, на основе которых извещатель принимает решение о состоянии контролируемой зоны, могут быть охарактеризованы матрицей строкой

$$\mathbf{U}^i_{jm} = \left[u^i_{jm1}(t),\ldots u^i_{jmn}(t),\ldots \quad u^i_{jmN}(t)\right], \text{ где } j = 1\ldots J; \quad m = 1\ldots M^i_j; \quad n = 1\ldots N. \tag{1}$$

Элементы этой матрицы характеризуют *n*-ю информационную характеристику или параметр объекта, контролируемые *m*-м извещателем *j*-о шлейфа *i*-й ЛССОИ. Для общего случая нескольких извещателей в шлейфе имеем трехмерную матрицу $\mathbf{U}^i$ информационных параметров, строки которой определяются последним выражением. То есть $\mathbf{U}^i$ определяет трехмерное пространство состояний устройств обнаружения угроз – извещателей i–й подсистемы.

Например, пусть имеется контрольная панель с двумя шлейфами, в один из которых включены два пассивных инфракрасных (ПИК) извещателя и во второй – один комбинированный. ПИК извещатели контролируют два параметра – интенсивность ИК излучения и количество превышений порога, а комбинированные – три (интенсивность ИК излучения, доплеровский сдвиг частоты и временной интервал между превышением порога этими параметрами). Тогда для рассматриваемого примера матрица $\mathbf{U}$ будет иметь вид

$$\mathbf{U} = \begin{bmatrix} & & \begin{bmatrix} 0 & 0 \\ u_{213}(t) & 0 \end{bmatrix} \\ & \begin{bmatrix} u_{112}(t) & u_{122}(t) \\ u_{212}(t) & 0 \end{bmatrix} & \\ \begin{bmatrix} u_{111}(t) & u_{121}(t) \\ u_{211}(t) & 0 \end{bmatrix} & & \end{bmatrix}. \tag{2}$$

В этой матрице $u_{111}(t)$, $u_{112}(t)$ и $u_{121}(t)$, $u_{122}(t)$ – параметры, контролируемые соответственно первым и вторым ПИК извещателями, а $u_{211}(t)$, $u_{212}(t)$ и $u_{213}(t)$ – комбинированным извещателем.

Анализ характеристик $u^i_{jmn}(t)$ по определенному алгоритму позволяет осуществить обнаружение угроз охраняемому объекту. Пусть $\mathbf{\Psi}\{\bullet\}$ – алгоритм формирования решения на уровне извещателей (УОУ). Так в рассматриваемом примере для комбинированного извещателя строка $u_{211}(t)$, $u_{212}(t)$, $u_{213}(t)$ должна преобразовываться по алгоритму, приведенному в [3] с использованием операции логического умножения $\cap$

$$u_{211}(t_1) \geq U_{01} \cap u_{212}(t_2) \geq U_{02} \cap u_{213}(t) = t_1 - t_2 \leq T_0. \quad (3)$$

То есть для принятия решения о том, что извещатель находится в состоянии тревоги, необходимо одновременное выполнение трех условий (3).

В частном случае одного извещателя в шлейфе *M*=1 (частном, но практически широко распространенном и, более того, являющимся желательным, а то и обязательным для систем высокой категории надежности) трехмерная матрица вырождается в двумерную

$$\mathbf{U}^i = \begin{bmatrix} u^i_{11}(t) & \dots & u^i_{1N}(t) \\ \dots & u^i_{jn}(t) & \dots \\ u^i_{J1}(t) & \dots & u^i_{JN}(t) \end{bmatrix}, \quad (4)$$

где строки матрицы соответствуют шлейфу или, что в данном случае то же самое, извещателю.

Трехмерная матрица (2) может быть преобразована в двумерную матрицу состояния извещателей по алгоритму преобразования $\mathbf{\Psi}\{\bullet\}$. Тогда, в результате преобразования, формируется двумерная матрица состояний УОУ *i*-й ЛССОИ

$$\mathbf{\Psi}^i\left\{\mathbf{U}^i_j\right\} = \mathbf{C}^i. \quad (5)$$

В результате получаем матрицу состояний извещателей

$$\mathbf{C}^i = \begin{bmatrix} c_{11}(t) & \dots & c_{1M}(t) \\ \dots & c_{jm}(t) & \dots \\ c_{J1}(t) & \dots & c_{JM}(t) \end{bmatrix} \quad (6)$$

с числом столбцов $M^i = \max\limits_{j=1,J}(M^i_j)$, равным максимальному количеству извещателей в каком-либо шлейфе и определяющую состояния нижнего системного уровня – извещателей. Алгоритм формирования элемента этой матрицы может быть записан как

$$c_{jm}(t) = \Psi_{jm}\left\{\psi_{jm1}\left\langle u_{jm1}(t)\right\rangle, \dots \quad \psi_{jmn}\left\langle u_{jmn}(t)\right\rangle, \dots \quad \psi_{jmN}\left\langle u_{jmN}(t)\right\rangle\right\}. \quad (7)$$

В частности, формула (3) является примером использования последнего выражения.

Для наиболее распространенного класса неадресных систем элементы матрицы $\mathbf{C}$ представляют собой дискретную функцию времени. Для другого класса, адресно-аналоговых систем, это будет непрерывная функция времени.

В свою очередь для наиболее типичного случая использования извещателей с информативностью 2 (состояния – НОРМА и ТРЕВОГА) элементы $c_{jm}(t)$ матрицы $\mathbf{C}$ принимают значения 0 либо 1. В другом частном случае выражения (4) матрица $\mathbf{C}$ вырождается в матрицу столбец

$$\mathbf{C}^i = \begin{bmatrix} c_1(t) \\ \dots \\ c_j(t) \\ \dots \\ c_J(t) \end{bmatrix} \quad (8)$$

состояний извещателей или, что в данном случае то же самое, шлейфов.

Далее ЛССОИ на основе анализа состояния УОУ в соответствии с алгоритмом принятия решений $\mathbf{\Phi}\{\bullet\}$ формирует матрицу $\mathbf{S}$ состояний следующего системного уровня – шлейфов ЛССОИ

$$\mathbf{S}^i = \mathbf{\Phi}^i\left\{\mathbf{C}^i\right\}. \quad (9)$$

В типичном случае при независимых шлейфах и информативности извещателя 2 алгоритм (9) имеет вид $\mathbf{S}^i = \mathbf{C}^i \cdot \mathbf{E}$, где матрица $\mathbf{C}$ определяется выражением (6), матрица столбец

$$\mathbf{E} = \begin{bmatrix} 1 \\ 1 \\ \dots \\ 1 \end{bmatrix} \text{ имеет } j \text{ единичных строк и, следовательно, } \mathbf{S}^i = \begin{bmatrix} s_1(t) \\ \dots \\ s_J(t) \end{bmatrix}, \tag{10}$$

то есть $s_j = \sum_{m=1}^{M} c_{jm}(t)$. Соответственно решение принимается по правилу

$$s_j(t) \geq Q, \tag{11}$$

где $j = 1,...,J$, а значение порога Q определяется количеством извещателей в шлейфе, которые должны зафиксировать угрозу. Обычно $Q = 1$ – при фиксации угрозы по одному извещателю. Для частного случая (8) матрицы $\mathbf{C}^i$ и $\mathbf{S}^i$ совпадают. В рассматриваемом примере элементы s_j принимают значения 1 (тревога) или 0 (норма).

Учет того или иного состояния извещателей для оценки состояния ЛССОИ должен проводиться в общем случае на основе режима работы последней. В свою очередь режим работы ЛССОИ может быть учтен соответствующей матрицей режимов работы шлейфов

$$\mathbf{P}^i = \left[p_1,..., p_j,..., p_J\right].$$

Значения элементов последней матрицы зависят от режима работы соответствующего шлейфа (1 – охрана, 0 – снято с охраны).

С учетом этого матрица состояний $\mathbf{S}^i$ должна определяться как

$$\mathbf{S}^i = \left(\mathbf{1} \cdot \mathbf{P}\right) \cdot \mathbf{\Phi}^i\left\{\mathbf{C}^i\right\}, \text{ где } \mathbf{1} \text{ – единичная матрица размером } J \times J.$$

Результатом сравнения по правилу (11) будет матрица столбец решений о состоянии шлейфов $\mathbf{R}^i$ с элементами r_j среднего уровня СБ ЛССОИ

$$\mathbf{R}^i = \left[r_1,...,r_j,...,r_J\right]^T.$$

Заметим, что в более сложном варианте, например, подтверждения тревоги (повторное срабатывание за определенный временной интервал или пересекающихся зон) алгоритм обработки естественно усложняется. Так, в частности, в случае двойного срабатывания значение порога $Q = 2$.

Во втором случае (пересекающихся зон) необходима совместная обработка нескольких (соответствующих) строк матрицы (6) состояния извещателей. Для этого введем матрицу пересечений зон

$$\mathbf{\Pi}^i = \begin{bmatrix} \pi_{11} & \dots & \pi_{J1} \\ \dots & \pi_{kj} & \dots \\ \pi_{1K} & \dots & \pi_{JK} \end{bmatrix}, \tag{12}$$

в которой ее элементы π_{kj} принимают значения 0 или 1, $k = 1,...,K$, а K равно количеству групп пересекающихся шлейфов. Положение единичных элементов π_{kj} строк матрицы $\mathbf{\Pi}^i$ определяет собственно пересекающиеся зоны для каждой k-й группы шлейфов. Соответственно в этом случае

$$\mathbf{R}^i = \mathbf{\Pi}^i \cdot \left(\mathbf{\Phi}\left\{\mathbf{C}^i\right\}\right), \text{ или в рассматриваемом примере } \mathbf{R}^i = \mathbf{\Pi}^i \cdot \left(\mathbf{C}^i \cdot \mathbf{E}\right) \tag{13}$$

с аналогичным правилом принятия решения $r_j(t) \geq Q_k$ при значении порога, равном количеству пересекающихся зон.

Таким образом, окончательно столбцы двухмерной матрицы $\mathbf{P}$ состояний системы безопасности в целом определяются матрицами столбцами состояния локальных подсистем, равных

$$\mathbf{R}^i = \mathbf{\Pi}^i \cdot \left(\mathbf{1} \cdot \mathbf{P}^i\right)\left(\mathbf{\Phi}^i\left\langle\mathbf{\Psi}^i\left\{\mathbf{U}_j^i\right\}\right\rangle\right).$$

Предполагая без потери общности, что ЛССОИ являются подсистемами комплексной или интегрированной системы безопасности и выполняют различные задачи, можно считать, что состояние тревоги имеет место при выполнении $p_{ij} \geq Q_{ij}$, где значение порога определяется алгоритмом работы ЦССОИ.

Заметим, что в общем случае должны быть введены временные окна анализа состояния УОУ при принятии решения на среднем уровне СБ – ЛССОИ.

Кроме того, зачастую необходимо учитывать приоритетность тех или иных событий в системе, точнее приоритетность реакции системы противодействия и ликвидации угроз на решения отдельных уровней системы по обнаружению угроз защищаемому объекту. В общем случае порядок приоритетов может не совпадать с порядком системных уровней. Разные события на одном уровне могут иметь разный приоритет и, наоборот, события на разных уровнях – одинаковый приоритет.

Литература: 1. В. В. Волхонский. Устройства охранной сигнализации. Изд. 2 допол. и перераб. Экополис и культура. СПб., 2000, 312 с. 2. Волхонский В. В. Системы охранной сигнализации. Экополис и культура, СПб, 2000, 164 с. 3. Волхонский В. В. Устройства охранной сигнализации. Часть 1. Извещатели. Изд. 3 допол. и перераб. Экополис и культура, СПб, 2001, 239 с.

УДК 621.395, 621.391.82

МЕТОД ЗАХИСТУ ЦІЛІСНОСТІ ІНФОРМАЦІЇ, ЩО ПЕРЕДАЄТЬСЯ В СИСТЕМАХ АБОНЕНТСЬКОГО РАДІОДОСТУПУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Олександр Корнейко, Олексій Кувшинов, Сергій Лівенцев

Військовий інститут телекомунікацій та інформатизації НТУУ "КПІ"

Анотація: **Запропоновано метод забезпечення цілісності інформації в системах абонентського радіодоступу спеціального призначення з псевдовипадковим перестроюванням робочої частоти. В основу методу покладено структурну адаптацію системи передачі інформації. Наведені рекомендації з побудови захищених систем абонентського радіодоступу. Отримані аналітичні вирази дозволяють визначити ступінь руйнування цілісності інформації, переданої в системах зв'язку спеціального призначення в умовах впливу найгірших завад.**

Summary: **In this task was offered the method of maintenance of integrity of the information in systems of user's radioaccess of special purpose with pseudo-casual reorganization of working frequency. In a basis of a method was fixed the structural adaptation of system of transfer of the information. There were given the recommendations from construction of the protected systems of user's radioaccess. In this fask were received the analytical expressions allowing to define a degree of destruction of integrity of the information transferred in systems of communication of special purpose in conditions of influence of the worst handicapes.**

Ключові слова: **Цілісність, захищеність, інформація, абонентський радіодоступ, псевдовипадкове перестроювання робочої частоти (ППРЧ), навмисні завади.**

I Вступ

Інформаційна безпека відіграє важливу роль у забезпеченні життєво важливих інтересів будь-якої держави. Створення розвинутого і захищеного інформаційного середовища є невід'ємною умовою розвитку суспільства. Поряд з цим необхідно створення систем керування, які забезпечують мінімальний ризик інформації, що пов'язаний з можливістю нанесення збитків власникам інформації (державі, юридичним особам усіх форм власності і громадянам) у результаті впливу природних і навмисних завад, незаконного її одержання і/або спотворення.

Розвиток захищеного радіозв'язку є невід'ємною частиною підвищення ефективності систем керування і передачі інформації рухомим об'єктам. Радіозв'язок характеризується зростаючими потребами в обміні цифровою інформацією з мобільними і віддаленими абонентами, які у сукупності утворюють територіально розподілені інформаційно-обчислювальні й інформаційно-керуючі мережі.

Актуальність застосування захищених радіомереж пояснюється об'єднанням переваг системи радіозв'язку, яка має загальне середовище поширення радіохвиль для всіх користувачів, з перевагами інформаційних мереж з комутацією повідомлень, заснованих на розгалуженій обчислювальній інфраструктурі.