УДК 004.273:004.056

Д. О. Маркин, сотрудник, e-mail: admin@nikitka.net, **В. В. Комашинский,** канд. техн. наук, доц.,
И. Ю. Баранов, канд. техн. наук, доц.,
Академия ФСО России, г. Орел

Модель управления профилем защиты мобильного устройства при доступе к услугам с разным уровнем конфиденциальности

Описана модель процесса управления логической структурой мобильного устройства, дана характеристика логической структуры мобильного устройства, показано ее место в системе управления доступом к услугам с разным уровнем конфиденциальности, описана модель логической структуры взаимосвязей между функциональными блоками мобильного устройства, а также модель управления профилем защиты мобильного устройства при доступе к услугам с разным уровнем конфиденциальности на основе матричных графовых грамматик.

Ключевые слова: *мобильное устройство, профиль защиты, реконфигурация логической структуры, динамические графы, графовые грамматики*

Введение

Современный мобильный телефон, как и достаточно широкий спектр мобильных устройств (МУ), обладающих и вычислительными, и коммуникационными ресурсами, представляет собой медиаустройство для повседневной работы и развлечений, где функция телефонных переговоров не является первостепенно важной [1]. Для улучшения показателя экономичности основные узлы современных МУ агрегированы в составе микросхемы класса SoC (System-on-Chip, система на чипе), на которую возлагается весь перечень задач сбора, обработки, хранения и обмена пользовательской и служебной информацией [2]. Такая SoC зачастую объединяет на одном кристалле несколько ядер процессора, коммуникационный процессор (baseband processor), графический сопроцессор и др. Добавление при необходимости микроконтроллеров для кодирования речи, высокочастотных блоков для работы в различных стандартах сети сотовой связи, интерфейсных блоков Wi-Fi сети, модулей GPS/ГЛОНАСС, а также набор интерфейсов для взаимодействия с различными типами устройств (USB, SD, MMC, UART и др.) обеспечивает конфигурирование МУ для разных уровней рынка и требований пользователей и обеспечивает многофункциональность МУ.

В то же время на современном этапе развития телекоммуникационных и вычислительных инфраструктур часто возникает задача обеспечения информационного взаимодействия между специализированными информационно-телекоммуникационными ресурсами (ИТ-ресурсами), обладающими различным уровнем конфиденциальности, и выполнения требований по защите информации. На данный момент эта задача в отношении МУ не решена по ряду различных причин, в том числе технологических и нормативно-правовых. Однако, учитывая современный уровень развития технологий проектирования МУ и существующие тенденции, объективно можно построить МУ с управляемой логической структурой взаимосвязей функциональных блоков или модулей на микросхеме класса SoC таким образом, чтобы при необходимости обмена информационными потоками разного уровня конфиденциальности формировалась такая логическая структура МУ, при которой данные потоки, с одной стороны, не пересекались бы, а с другой — были защищены с помощью средств защиты информации на аппаратном уровне МУ. Своеобразным прототипом подобного решения могут служить принципы построения современных программируемых радиостанций, рассмотренных в работах [3, 4].

В данной работе предлагается формальная модель управления профилем защиты (ПЗ) единого многофункционального мобильного устройства (ММУ) при доступе к разнокатегорированным услугам (услугам с разным уровнем конфиденциальности), основанная на изменении логической структуры трактов прохождения информационных потоков. Сущность управления профилем защиты в ММУ заключается в реконфигурации логической структуры взаимосвязей между функциональными блоками ММУ таким образом, чтобы передача информационных потоков с различным уровнем конфиденциальности осуществлялась с выполнением требований по защите информации автоматизиро-

ванно либо автоматически в зависимости от уровня конфиденциальности передаваемой информации. Пример решения подобной задачи в отношении интегрированных объектов информатизации описан в работе К. М. Зорина [5]. Основой предложенного Зориным подхода по реконфигурации логической структуры является обеспечение эффективного функционирования искусственного интеллекта как средства передачи информации, однако вопросы управления логической структурой ММУ как объекта информатизации [6], обеспечивающего защищенное сетевое взаимодействие с помощью информационных потоков с разным уровнем конфиденциальности, в данной работе не рассматриваются. В описываемой модели управления профилем защиты ММУ при доступе к разнокатегорированным услугам предлагается распространить идеи реконфигурации логической структуры искусственного интеллекта на логическую структуру взаимосвязей между функциональными блоками ММУ, чтобы обеспечить безопасный обмен информационными потоками с разным уровнем конфиденциальности между объектами информатизации.

Общий вид модели процесса управления логической структурой мобильного устройства и формальная постановка задачи

Описание изменяемой логической структуры ММУ как информационной системы (ИС) может быть представлено как последовательность задач синтеза на каждом этапе функционирования. В этом случае функционирование ММУ может быть описано динамическими моделями [7, 8]. Таким образом, динамическая модель описания ММУ рассматривает процедуры синтеза его логической структуры в каждый момент времени и с учетом его поведения в предыдущие моменты времени.

В контексте данной работы понятия профиля защиты ММУ и логическая структура ММУ являются синонимичными и характеризуют взаимосвязи между функциональными блоками ММУ, определяющие тракты прохождения информационных потоков с разным уровнем конфиденциальности. В контексте управления профилем защиты при доступе к услугам с разным уровнем конфиденциальности целями изменения состояния ММУ (его логической структуры) является обеспечение безопасного информационного обмена между ММУ и защищенной информационной инфраструктурой. Решение о реконфигурации ММУ принимает некоторая подсистема управления на основе результатов наблюдения за ним, которое заключается в выборе альтернативных управляющих воздействий — альтернативных логических структур ММУ. Очевидно, что каждая логическая структура ММУ отличается от других по целому ряду параметров, таких как быстродействие, надежность, пропускная способность и, самое главное, защищенность. Данные параметры могут выступать в качестве критериев оценивания того или иного управляющего воздействия для приведения логической структуры ММУ в оптимальное состояние для текущих условий.

В общем случае целью изменения структуры ММУ является достижение заданных требований надсистемы или, иными словами, выполнение требований по защите информации вследствие возникновения внутренних факторов или ограничений (возникновения необходимости передачи информации с иным уровнем конфиденциальности).

В общем случае процесс управления конфигурацией ММУ может быть представлен в виде следующих выражений.

Состояния $S(t)$ моделируемого ММУ зависят от случайных воздействий $\xi_S(t)$ и процессов управления $x(t)$:

$$S(t) = F\{x(\tau_1), \xi(\tau_2), t\}, \tau_1, \tau_2 \in [t_0, t] \cap T. \quad (1)$$

Каналы мониторинга можно описать процессом

$$S_U(t) = F_{S_U}\{S(\tau_1), \xi_{S_U}(\tau_2), t\},$$

где $\xi_{S_U}(t)$ — стохастический порождающий процесс, определяющий случайный характер мониторинга.

Системы принятия решений задаются стохастическими функционалами, вырабатывающими в каждый момент времени t рандомизированные значения $u(t)$ принятых решений по наблюдениям $S_U(t)$ при $\tau \in [t_0, t] \cap T$:

$$u(t) = F_U\{S_U(\tau_1), \xi_U(\tau_2), t\},$$

где $\xi_U(t)$ — стохастический порождающий процесс, определяющий рандомизацию решений $u(t)$.

Канал управления характеризуется процессом управления $x(t)$ в зависимости от принятых решений:

$$x(t) = F_x\{u(\tau_1), \xi_x(\tau_2), t\}, \quad (2)$$

где $\xi_x(t)$ — стохастические порождающие процессы, определяющие случайный характер реконфигурации.

Таким образом, для моделирования необходимо определить вектор анализируемых показателей эффективности и приведенные ранее функционалы, определяющие динамику состояний ММУ при известном начальном состоянии, а также интерпретировать характеристики и параметры функционалов значениями, характеризующими реальное ММУ.

Характеристика логической структуры многофункционального мобильного устройства

Для построения модели управления ПЗ ММУ необходимо конкретизировать характеристику ММУ и его структуру. Суть реконфигурации логической структуры ММУ будет заключаться в воздействии на структурные элементы ММУ в целях повышения эффективности функционирования с учетом обеспечения требуемого уровня безопасности информационного взаимодействия. Пример типичной структуры ММУ, существующей на современном этапе развития, представлен на рис. 1.

Важно отметить, что при работе ММУ в режиме обработки конфиденциальной информации могут предъявляться дополнительные требования, заключающиеся в необходимости отключения ряда функциональных блоков ММУ, создающих предпосылки или возможность утечки информации.

Задачи формирования необходимой логической структуры трактов прохождения информационных потоков в ММУ могут возлагаться на аппаратно-программный модуль доверенной загрузки, а команда на выполнение изменения логической структуры ММУ в целях создания необходимых условий для обработки информации с заданным уровнем конфиденциальности (т. е., по сути, на выполнение реконфигурации ММУ) может поступать по каналу управления, использующего, например, корпоративную защищенную беспроводную локально-вычислительную сеть на базе технологии Wi-Fi, состоящую из доверенных точек доступа и контроллера беспроводной сети. Таким образом, инфраструктура системы управления профилем защиты ММУ может выглядеть так, как представлено на рис. 2.

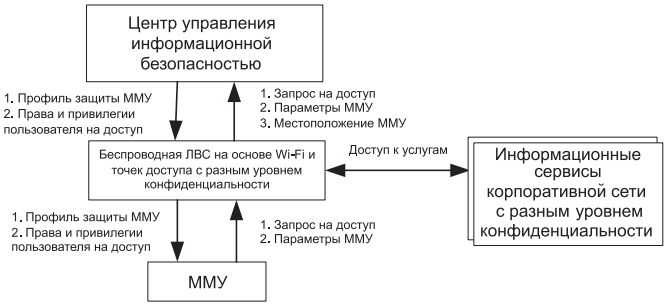

Рис. 2. Обобщенная схема инфраструктуры управления ПЗ ММУ при доступе к услугам с уровнем конфиденциальности

Задача формирования профиля защиты ММУ возлагается на центр управления информационной безопасностью. Опишем формальную модель логической структуры взаимосвязей между функциональными блоками ММУ, которая является объектом управления.

Формальное описание модели логической структуры взаимосвязей между функциональными блоками мобильного устройства

Модель логической структуры ММУ может быть представлена в виде совокупности функциональных блоков, обеспечивающих передачу информационных потоков, которую можно обозначить выражением

$$B = \{b_i^k\},$$

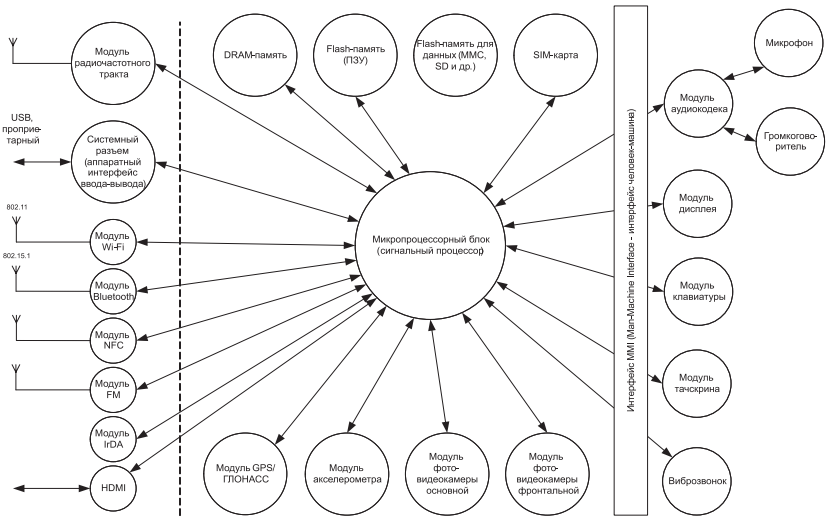

Рис. 1. Схема логической структуры взаимосвязей между функциональными блоками многофункционального мобильного устройства

где $i = \overline{1, N_B}$, N_B — число функциональных блоков (компонентов) ММУ; $k = \overline{1, N_t}$, N_t — число типов интерфейсов функциональных блоков. Для более полного и общего учета возможностей передачи информационных потоков дополнительно может быть определено число режимов работы каждого типа интерфейса $l(k)$.

На основе данных параметров можно определить варианты трактов прохождения информационных потоков через ММУ с использованием индикатора возможности установления связи между i-м и j-м функциональными блоками:

$$I_{i,j}^{k,l} = \{0, 1\},\ i, j = \overline{1, N_B},\ k = \overline{1, N_t},\ l = l(k).$$

В случае $I_{i,j}^{k,l} = 1$ связь между функциональными блоками существует, в противном случае — нет. Данные величины отражают наличие информационных направлений между компонентами ММУ.

Дополнительно, с учетом наличия различных типов интерфейсов, может быть учтен показатель связности $f^{k,l}$, обеспечиваемый k-м типом интерфейса в l-м режиме работы. Показатель связности подразумевает наличие связи один к одному, одни ко многим или многие ко многим.

Математическое описание маршрутов передачи информационного потока через компоненты ММУ может быть представлено в виде некоторого множества M, учитывающего наличие информационных направлений между компонентами. Матричное представление маршрута будет иметь вид

$$m = \begin{bmatrix} i_1 & \dots & i_{L_m-1} & i_{L_m} \\ k_1 & \dots & k_{L_m-1} & 0 \\ l_1 & \dots & l_{L_m-1} & 0 \end{bmatrix},$$

где L_m — общее число функциональных блоков, входящих в маршрут m с длиной $L_m - 1$; $(i_1, ..., i_{L_m})$ —

последовательность интерфейсов ММУ в маршруте; $(k_1, ..., k_{L_m - 1})$ — последовательность типов интерфейсов в маршруте; $(l_1, ..., l_{L_m - 1})$ — последовательность режимов работы соответствующих типов интерфейсов в маршруте. В соответствии с этим множество M определяет допустимые маршруты передачи информационных потоков.

С использованием данной матрицы маршрута информационного потока может быть получен индикатор действующего маршрута в виде выражения

$$I_m = I_{i_1, i_2}^{k_1, l_1}, I_{i_2, i_3}^{k_2, l_2}, ..., I_{i_n, i_{n+1}}^{k_n, l_n} I_{i_1} I_{i_2} ... I_{i_{n+1}}, \quad n = L_m - 1. \tag{3}$$

Таким образом, состояние логической структуры ММУ, обслуживающей информационные потоки с разным уровнем конфиденциальности, в соответствии с выражением (1) в каждый момент времени t задается вектором массивов:

$$s^{<0>}(t) = \langle \{I_i(t)\}, \{b_i^k(t)\}, \{I_{i,j}^{k,l}(t)\}, \{f^{k,l}\}, M \rangle,$$

где I_i, $i = \overline{1, N_B}$, — индикатор существования функционального блока (компонента) ММУ; M и $f^{k,l}$ — исходные данные.

Процесс реконфигурации $x^{<0>}(t)$ логической структуры ММУ, представленный в общем виде выражением (2), заключается в управлении параметрами (составом) ММУ. Такое управление можно задать массивом $\{b_{xi}^k(t)\}$, где $b_{xi}^k(t)$ — число интерфейсов k-го типа, введенных на i-й функциональный блок за промежуток времени (t_0, t), т. е.

$$x^{<0>}(t) = \langle b_{xi}^k(t) \rangle. \tag{4}$$

Процесс управления логической структурой ММУ в общем виде задается выражением (2) и заключается в реконфигурации структуры данной ММУ, определяемой выражением (4). Реальное поведение логической структуры ММУ примет вид

$$b_{i,j}^{k,l}(t) = b_{xi,j}^{k,l}(t) I_{i,j}^{k,l}(t) I_i(t) I_j(t).$$

Связность линий между функциональными блоками ММУ в каждый момент времени t может быть определена в виде

$$f^{k,l} = f^{k,l}(t) b_{i,j}^{k,l}(t),$$

а также может быть представлена в виде матрицы связности функциональных блоков ММУ:

$$F^{k,l}(t) = [f^{k,l}] = [f^{k,l}(t) \cdot b_{i,j}^{k,l}(t)],$$

определяющей допустимые маршруты прохождения информационных потоков в рамках информационной инфраструктуры логической структуры ММУ на момент времени t.

Если перейти от представления логической структуры ММУ в виде наличия в ее составе заданных функциональных блоков с их интерфейсами и режимами работы к представлению в виде связности между данными блоками, то тогда процесс реконфигурации логической структуры ММУ и, соответственно, процесс управления информационными потоками может быть представлен в виде выражения

$$x^{<2>}(t) = \{f_x(m, t)\}.$$

Тогда в общем виде процесс поведения логической структуры в виде динамики изменения связности между функциональными блоками ММУ и с учетом случайных воздействий на нее примет вид

$$f(m, t) = [f_x(m, t) - f_{\xi_S}(m, t)] I(m, t),$$

где $I(m, t)$ — индикатор действующего маршрута m в момент времени t, представленный выражением (3).

На основе представленных выражений можно сделать вывод, что процесс управления профилем защиты ММУ является управлением логической структурой, представленной в виде связности между функциональными блоками ММУ. Таким образом, на центр управления информационной безопасности возлагается задача выбора оптимальной матрицы связности функциональных блоков ММУ (профиля защиты ММУ), обеспечивающего защищенный доступ к разнокатегорированным услугам корпоративной сети, исходя из текущих условий и параметров доступа.

Модель управления профилем защиты мобильного устройства на основе матричных графовых грамматик

Задачей управления информационными потоками с разным уровнем конфиденциальности является адаптация логической структуры ММУ до такого состояния, при котором будут выполняться требования по обеспечению безопасной передачи информационных потоков через функциональные блоки ММУ, а также ряд других требований, предъявляемых той или иной надсистемой. В общем виде процесс адаптации может быть представлен как последовательность улучшающихся структур:

$$W_i, W_{i+1}, ..., W_N, i = \overline{1, N}, W = \{W_i\},$$

где W — множество допустимых логических структур ММУ; W_i — логическая структура ММУ на i-й итерации; N — число итераций, при этом на каждой итерации выполняется условие

$$W_N \succ W_{N-1} \succ ... \succ W_{i+1} \succ W_i,$$

т. е. некоторая логическая структура ММУ на $(i + 1)$-й итерации предпочтительней (лучше) структуры на предыдущей i-й итерации процесса адаптации.

Стоит отметить, что наиболее подходящим формальным описанием изменения логической структуры ММУ, которое выражается, в том числе, в виде

изменения маршрутов информационных потоков, является теория графов. Функциональные блоки логической структуры ММУ в этом случае представляются в виде вершин графа, а ребра графа — направления трактов прохождения информационных потоков.

Наиболее подходящим аппаратом для описания процесса генерации (эволюционной адаптации) структуры являются графовые грамматики, которые делятся на порождающие и трансформирующие. Порождающая графовая грамматика содержит конечное множество исходных графов и конечное множество правил допустимых локальных преобразований графов. Если набор исходных графов не задан, грамматика называется трансформирующей. Для решения подобных задач анализа и синтеза динамических структур, описываемых графами, в 70-х—80-х гг. советскими учеными была разработана теория "графодинамики" [9—11].

В 2007 г. для описания динамики графа и описания графовых грамматик был разработан (в основном на булевой алгебре и алгебре матриц) строгий алгебраический подход, названный матричными графовыми грамматиками (Matrix Graph Grammars) [12].

В общем виде формальная грамматика задается в виде

$$G = (V_T,\ V_N,\ P,\ S),$$

где V_T — конечный алфавит нетерминальных символов — множество матриц, описывающих матрицы связности функциональных блоков логической структуры ММУ (исходные маршруты информационных потоков в ММУ); V_N — конечный алфавит терминальных символов — множество матриц, описывающих итоговые матрицы связности логической структуры ММУ (маршруты информационных потоков в ММУ); P — конечное множество правил порождения (допустимых операций над матрицами связности логической структуры ММУ); S — начальный нетерминал грамматики (исходная матрица связности функциональных блоков логической структуры ММУ (например, при включении питания)).

Опишем логическую структуру ММУ в терминах теории графов.

Любой граф можно представить матрицей смежности

$$A_G = \{a_{ij}\},$$

где $a_{ij} = 1$, если существует связь между i-м и j-м функциональными блоками.

Пусть L — исходный граф (перед шагом трансформации, т. е. $L \in V_T$), R — конечный граф (после шага трансформации, т. е. $R \in V_N$). Необходимо определить действие, преобразующее исходный граф L в R:

$$p(L,\ R)\colon L \to R,$$

где $p \in P = \Xi = (\xi_1, \xi_2, \ldots, \xi_p)$.

Суть преобразования графа заключается в удалении либо добавлении связей между вершинами графа, т. е. по сути в изменении матрицы связности $F^{k,\,l}$, поэтому введем понятие матрицы удаления связей и матрицы добавления связей.

Тогда матрица удаления связей может быть представлена в виде

$$e = L \wedge (\overline{L \wedge R}) = L \wedge \overline{R},\ e = (e)_{ij} =$$
$$= \begin{cases} 1, \text{ удаляется связь;} \\ 0, \text{ связь не удаляется,} \end{cases}$$

а матрица добавления связей в виде

$$r = R \wedge (\overline{L \wedge R}) = R \wedge \overline{L},\ r = (r)_{ij} =$$
$$= \begin{cases} 1, \text{ добавляется связь;} \\ 0, \text{ связь не добавляется.} \end{cases}$$

Теперь на основе данных выражений можно представить преобразование $p(L,\ R)\colon L \to R$ операций над исходной матрицей связности $L \in V_T \subseteq W$ и матрицами удаления и добавления связей:

$$p\colon L \to R \Rightarrow R = r \vee (\overline{e} \wedge L).$$

С помощью этого подхода можно синтезировать любой случайный граф. Чтобы получаемые в результате преобразования $p(L,\ R)\colon L \to R$ случайные графы описывали реальную структуру ММУ, необходимо задать ряд ограничений на преобразования графа, т. е. в терминах формальной грамматики правила порождения.

На рис. 3 представлен пример осуществления преобразования $p(L,\ R)\colon L \to R$ в случае с операцией полного дублирования вершины.

Матрица связности для исходного и конечного графов выглядит как

$$L = \left(\begin{array}{cccc|c} 0 & 0 & 0 & 1 & k \\ 0 & 0 & 0 & 1 & l \\ 0 & 0 & 0 & 1 & m \\ 1 & 1 & 1 & 0 & n \end{array}\right) = \left(\begin{array}{ccccc|c} 0 & 0 & 0 & 1 & 0 & k \\ 0 & 0 & 0 & 1 & 0 & l \\ 0 & 0 & 0 & 1 & 0 & m \\ 1 & 1 & 1 & 0 & 0 & n \\ 0 & 0 & 0 & 0 & 0 & z \end{array}\right),\ R = \left(\begin{array}{cccccc|c} 0 & 0 & 0 & 1 & 1 & k \\ 0 & 0 & 0 & 1 & 1 & l \\ 0 & 0 & 0 & 1 & 1 & m \\ 1 & 1 & 1 & 0 & 0 & n \\ 1 & 1 & 1 & 0 & 0 & z \end{array}\right).$$

Матрицы удаления и добавления связей —

$$e = \left(\begin{array}{ccccc|c} 0 & 0 & 0 & 0 & 0 & k \\ 0 & 0 & 0 & 0 & 0 & l \\ 0 & 0 & 0 & 0 & 0 & m \\ 0 & 0 & 0 & 0 & 0 & n \\ 0 & 0 & 0 & 0 & 0 & z \end{array}\right),\ r = \left(\begin{array}{ccccc|c} 0 & 0 & 0 & 0 & 1 & k \\ 0 & 0 & 0 & 0 & 1 & l \\ 0 & 0 & 0 & 0 & 1 & m \\ 0 & 0 & 0 & 0 & 0 & n \\ 1 & 1 & 1 & 0 & 0 & z \end{array}\right).$$

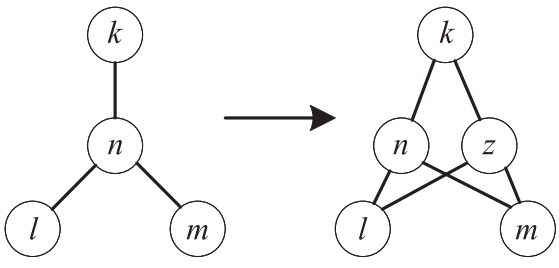

Рис. 3. Полное дублирование вершины

Все преобразования имеют вид

$$L = \left(\begin{array}{ccccc|c} 0&0&0&1&0&k\\ 0&0&0&1&0&l\\ 0&0&0&1&0&m\\ 1&1&1&0&0&n\\ 0&0&0&0&0&z \end{array}\right) \vee \left[\left(\begin{array}{ccccc} 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1\\ 1&1&1&1&1 \end{array}\right) \wedge \right.$$

$$\left. \wedge \left(\begin{array}{ccccc} 0&0&0&0&1\\ 0&0&0&0&1\\ 0&0&0&0&1\\ 0&0&0&0&0\\ 1&1&1&0&0 \end{array}\right)\right] = \left(\begin{array}{ccccc|c} 0&0&0&1&1&k\\ 0&0&0&1&1&l\\ 0&0&0&1&1&m\\ 1&1&1&0&0&n\\ 1&1&1&0&0&z \end{array}\right).$$

Аналогичным образом могут быть описаны и другие операции над графами, такие как понижение степени вершины, повышение степени вершины, понижение степени вершины разбиением, понижение размерности задачи путем разбиения графов и т. д.

Также различные комбинации отдельных подобных правил могут быть объединены в последовательности преобразований [12].

Теперь, на основе описания с помощью матричных графовых грамматик процедуры управления логической структурой ММУ, влияющей на маршруты информационных потоков, можно определить процесс адаптации логической структуры ММУ в соответствии с заданными критериями. В общем виде процесс адаптации может быть представлен в виде рекуррентного соотношения

$$c^i_{n+1} = c^i_n + \gamma_n Q_i(c_n, X_n),$$

где $c_n = \{c^i_n\}$ — параметры, характеризующие качество структуры по заданным критериям; X_n — случайная величина (некоторый граф, представляющий логическую структуру ММУ в момент n); Q_i — детерминированная функция, определяющая качество логической структуры ММУ; γ_n — числовая последовательность, определяющая преобразования из множества $\Xi = (\xi_1, \xi_2, ..., \xi_p)$.

Для решения задачи адаптации может быть использован адаптивный алгоритм [15]

$$c_n = c_{n-1} - \gamma_n \frac{dQ(c_{n-1}, X_n)}{dc}.$$

Вероятность сходимости данной рекуррентной последовательности, как показано в работах [13, 14], равна единице при выполнении следующих условий:

$$\sum_{n=1}^{\infty} \gamma_n = \infty, \quad \lim_{n\to\infty} \gamma_n = 0;$$

$$\inf_{\delta < (c - c^*) < \frac{1}{2}} M_x\left\{(c - c^*)\frac{dQ(X, c)}{dc}\right\} > 0, \ \forall \varepsilon > 0;$$

$$M_x\left\{\left[\frac{dQ(X, c)}{dc}\right]^2\right\} \leqslant (1 + c^2), \ d > 0.$$

Ограничения, накладываемые ММУ на возможности по генерации логической структуры, приводят к тому, что траектория процесса аппроксимации не выходит за пределы множества допустимых значений, что делает доказательство сходимости итеративного процесса тривиальным.

Необходимо определить правила остановки для адаптационного алгоритма. Способ определения момента остановки — конечного значения номера итерации N — состоит в выборе по достаточно малым разностям между несколькими последовательными значениями c_{n-i+1}, c_{n-1}, $i = 1, ..., k$. Данное условие может быть записано в виде

$$N = \min\left\{n: \max_{i=\overline{1,k}} |c_{n-i+1} - c_{n-i}| < \delta\right\}$$

или

$$N = \min\left\{n: \sum_{i=1}^{k} |c_{n-i+1} - c_{n-i}| < \delta\right\},$$

где δ — некоторая величина, равная предельной допустимой разнице между последовательными значениями параметров, характеризующих качество оптимизируемой структуры.

Для обоснования правила остановки необходимо решить вопрос выбора:

$\delta(\varepsilon, \alpha)$, чтобы выполнялось

$$P\left(|c_n - c^*| < \frac{\varepsilon}{|c_n - c_{n-1}|} < \delta\right) \geqslant 1 - \alpha;$$

δ и k в зависимости от ε и α, чтобы выполнялось

$$P\left(|c_n - c^*| < \frac{\varepsilon}{\max\limits_{i=\overline{1,k}} |c_{n-i+1} - c_{n-i}|} < \delta\right) \geqslant 1 - \alpha$$

или

$$P\left(|c_n - c^*| < \frac{\varepsilon}{\sum\limits_{i=1}^{k} |c_n - c_{n-i}|} < \delta\right) \geqslant 1 - \alpha,$$

где c^* — решение задачи; k — число итераций; ε — величина, равная разнице между c_n и c^*; α — уровень значимости.

Конкретные значения параметров δ и k в зависимости от ε и α могут быть получены в результате моделирования процесса функционирования системы управления профилем защиты ММУ.

Заключение

В данной работе обоснована актуальность задачи управления информационными потоками с разным уровнем конфиденциальности при решении задач информационного взаимодействия различных информационных систем. Представлены общий вид

модели процесса управления логической структурой информационной системы и формальная постановка задачи. Дана характеристика логической структуры многофункционального мобильного устройства, обслуживающего информационные потоки с разным уровнем конфиденциальности.

Предложена модель управления информационными потоками с разным уровнем конфиденциальности на основе управления логической структурой информационной системы с использованием аппарата матричных графовых грамматик. Заданы критерии остановки адаптационного алгоритма, используемого для адаптации логической структуры информационной системы и поиска оптимальной.

Предложенная модель может быть использована при эксплуатации многофункциональных мобильных устройств в условиях защищенной корпоративной сети, в которой осуществляется обработка информации с разным уровнем конфиденциальности, а также в любых других условиях, когда окружающая обстановка требует изменения конфигурации логической структуры в целях оптимального расходования ресурсов одновременно с выполнением предъявляемых к устройству требований.

Список литературы

1. **Хрусталев Д. А.** Мобильные телефоны Siemens. Принципы устройства и ремонт. М.: Изумруд, 2004. 256 с.

2. **Заяц А.** Обзор и тестирование смартфона Caesar A9600, а также знакомство с MT6589 — четырехъядерной SoC MediaTek для бюджетных решений. URL: http://ixbt.com/md/pda/ (Дата обращения: 03.03.2014 г.).

3. **Щербак Н.** Программируемые радиостанции — будущее тактической связи // Электроника: Наука, Технология, Бизнес. 2001. № 5. С. 16—19.

4. **Uhm M.** Adaptivity in Action for SDR and Cognitive Radio // COTS Journal. February. 2006. URL: http://www.cotsjournalonline.com (Дата обращения: 14.10.2014 г.).

5. **Зорин К. М.** Модель и методика реконфигурации логической структуры интегрированного объекта информатизации // Известия СПбГЭТУ "ЛЭТИ". 2010. № 6. С. 20—25.

6. **ГОСТ Р 51275—2006.** Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Введ. 2006.12.27. М.: Федеральное агентство по техническому регулированию и метрологии, 2007. 8 с. (Национальный стандарт Российской Федерации).

7. **Чуднов А. М., Барашков П. Н., Ткаченко А. П., Ткаченко К. А.** Модель системы связи с управляемыми структурами в конфликтных условиях. Л.: ВАС, 1986.

8. **Советов Б. Я., Яковлев С. А.** Моделирование систем: учеб. для вузов. М.: Высшая школа, 2007.

9. **Петров С. В.** Графовые грамматики и задачи графодинамики // Автоматика и телемеханика. 1977. № 10.

10. **Петров С. В.** Нормальная форма графовых грамматик // Автоматика и телемеханика. 1977. № 6.

11. **Айзерман М. А., Гусев Л. А., Петров С. В., Смирнова И. М., Тененбаум Л. А.** Динамический подход к анализу структур, описываемых графами (основы графодинамики) // Сб. науч. трудов. Академия наук СССР "Исследовании по теории структур". М.: Наука, 1988.

12. **Perez P. P.** Matrix Graph Grammars: An Algebraic Approach to Graph Dynamics. VDM Verlag, 2009. С. 5—80.

13. **Браверман Э. М., Розоноэр Л. И.** Сходимость случайных процессов в теории обучения машин I, II // Автоматика и телемеханика, № 1. 1969.

14. **Цыпкин Я. З.** Адаптация и обучения в автоматизированных системах. М.: Наука. 1968.

15. **Ферманн Х. Х.** О некоторых подходах к определению правила остановки для алгоритмов адаптации // Проблемы случайного поиска. Кн. 4 / Под общ. ред. Л. А. Растригина. Рига: Зинатне, 1975. С. 55—59.

D. O. Markin, Employee, e-mail: admin@nikitka.net, **V. V. Komashinskij,** Associate Professor,
I. Yu. Baranov, Associate Professor, The Academy of the Federal security service of Russia

Mobile Device Security Profile Management Model Using Access to Services With Different Privacy Level

The article contains description of mobile device logical structure management process model. This model contains the analytic model of mobile device logical structure, the logical structure of mobile device functional blocks relations, the mobile device security profile management model based on matrix graph grammars.

The essence of mobile device logical structure management process model is the reconfiguration of the logical structure of the interconnections between the mobile device functional blocks such as CPU, RAM, communication modules, for example, GSM, CDMA, LTE, Wi-Fi, Bluetooth, video and audio subsystems, etc. The main objective of this model is providing the required level of information security.

Mobile device logical structure features are presented. These features allow to present informational traffic routes between mobile device functional blocks. So using these routes the mobile device logical structure can be justified.

The authors show location of this model in the services access control system using access to services with different privacy level. The optimal mobile device logical structure achieve by using the mathematical apparatus of dynamic graphs and optimization iterative algorithms.

Using this model the authors offer mobile device security profile management model using access to services with different privacy level based on matrix graph grammars.

Keywords: *mobile device, security profile, logical structure reconfiguration, dynamic graphs, graph grammars*

References

1. **Hrustalev D. A.** *Mobil'nye telefony Siemens. Principy ustrojstva i remont.* M.: Izumrud, 2004. 256 p.

2. **Zajac A.** *Obzor i testirovanie smartfona Caesar A9600, a takzhe znakomstvo s MT6589 — chetyrehiadernoi SoC MediaTek dlia biudzhetnyh reshenij.* URL: http://ixbt.com/md/pda/ (Data obrashhenija: 03.03.2014.).

3. **Shherbak N.** Programmiruemye radiostancii — budushhee takticheskoj svjazi / N. Shherbak. *Jelektronika: Nauka, Tehnologija, Biznes.* 2001, no. 5, pp. 16—19.

4. **Uhm M.** Adaptivity in Action for SDR and Cognitive Radio. *COTS Journal.* — February, 2006. URL: Rezhim dostupa: http://www.cotsjournalonline.com (Data obrashhenija: 14.10.2014).

5. **Zorin K. M.** Model' i metodika rekonfiguracii logicheskoj struktury integrirovannogo ob'ekta informatizacii. *Izvestija SPbGJeTU "LJeTI".* 2010, no. 6, pp. 20—25.

6. **GOST** R 51275—2006. *Zashhita informacii. Ob'ekt informatizacii. Faktory, vozdejstvujushhie na informaciju. Obshhie polozhenija. Vved.* 2006.12.27. — M.: Federal'noe agentstvo po tehnicheskomu regulirovaniju i metrologii, 2007. 8 p. (Nacional'nyj standart Rossijskoj Federacii).

7. **Chudnov A. M., Barashkov P. N., Tkachenko A. P., Tkachenko K. A.** *Model' sistemy svjazi s upravljaemymi strukturami v konfliktnyh uslovijah.* L.: VAS, 1986.

8. **Sovetov B. Ja., Jakovlev S. A.** Modelirovanie sistem: ucheb. dlja vuzov. M.: Vysshaja shkola, 2007.

9. **Petrov S. V.** Grafovye grammatiki i zadachi grafodinamiki. *Avtomatika i telemehanika.* 1977, no. 10.

10. **Petrov S. V.** Normal'naja forma grafovyh grammatik. *Avtomatika i telemehanika.* 1977, no. 6.

11. **Ajzerman M. A., Gusev L. A., Petrov S. V., Smirnova I. M., Tenenbaum L. A.** Dinamicheskij podhod k analizu struktur, opisyvaemyh grafami (osnovy grafodinamiki) / *Sb. nauch. trudov. Akademija nauk SSSR "Issledovanii po teorii struktur".* M.: Nauka, 1988.

12. **Perez P. P.** *Matrix Graph Grammars: An Algebraic Approach to Graph Dynamics.* VDM Verlag, 2009, pp. 5—80.

13. **Braverman Je. M., Rozonojer L. I.** Shodimost' sluchajnyh processov v teorii obuchenija mashin I, II / Je. M. Braverman. *Avtomatika i telemehanika.* 1969, no. 1.

14. **Cypkin Ja. Z.** *Adaptacija i obuchenija vavtomatizirovannyh sistemah.* M.: Nauka. 1968.

15. **Fermann H. H.** *O nekotoryh podhodah k opredeleniju pravila ostanovki dlja algoritmov adaptacii. Problemy sluchajnogo poiska.* Kn. 4. Pod obshh. red. L. A. Rastrigina. Riga: Zinatne, 1975, pp. 55—59.

УДК 004.942; 004.056.55; 004.384

Д. В. Капулин, канд. техн. наук., зав. каф., e-mail: dkapulin@sfu-kras.ru,
О. В. Дрозд, студент, e-mail: olvldrozd@gmail.com
Сибирский федеральный университет, г. Красноярск

Устройство аппаратного шифрования производственных данных

Предложено устройство, обеспечивающее защищенный обмен производственной информацией с использованием алгоритмов ГОСТ 28147—89. Реализация устройства выполнена с применением ПЛИС Xilinx Spartan-6. Подробно рассмотрены этапы проектирования устройства, проведено имитационное моделирование разработанного устройства в среде Simulink.

Ключевые слова: *аппаратное шифрование, передача данных, защита информации, беспроводная связь, wi-fi*

Введение

Широкое распространение технологий беспроводного *Ethernet* в корпоративном секторе и в секторе электронных устройств для частного пользования закономерным образом приводит к росту внимания к этим технологиям со стороны производителей и интеграторов автоматизированных систем управления технологическими процессами (АСУ ТП). Применительно к АСУ ТП беспроводные сети и устройства передачи данных обладают следующими преимуществами [1]:

- возможность расположения устройств приема-передачи в труднодоступных местах;
- удобство развертывания и обслуживания устройств;
- оперативное добавление устройств в корпоративную сеть или исключение из нее;
- возможность расположения устройств приема-передачи данных на подвижных объектах.

Кроме того, внедрение беспроводных устройств контроля технологических и производственных параметров открывает новые возможности по применению систем автоматики, такие как обеспечение доступа к объекту, контроль периметра объекта, наблюдение за перемещениями персонала на территории предприятия, автоматизация контроля проведения инспекций и технического обслуживания, контроль экологических параметров окружающей среды и т. д.

Разработку контрольно-измерительных приборов АСУ ТП со встроенными беспроводными интерфейсами ведет компания *Yokogawa* с использованием стандарта промышленной беспроводной связи ISA 100/11a. Номенклатура беспроводных измерительных преобразователей *Yokogawa* включает в себя датчики температуры, абсолютного, избыточного и дифференциального давления [2]. Среди производителей промышленных беспроводных точек дос-