DOI:

О ПРИМЕНЕНИИ ТЕОРЕТИКО-ГРУППОВЫХ И КОМБИНАТОРНЫХ МЕТОДОВ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЛОЖНЫХ СИСТЕМ

Максимовский А.Ю.

Институт проблем управления им. В.А. Трапезникова РАН, Россия, г. Москва
ул. Профсоюзная д.65
maximay62@ipu.ru

Аннотация: В докладе приведены результаты исследования алгебраических и комбинаторных свойств предложенной общей конструкции автоматных моделей сетевых объектов на основе регистра сдвига, которые позволяют оценить эффективность применения представленных методов и сценариев мониторинга информационной безопасности сетевых объектов и оптимизировать выбор используемых для этого средств.

Ключевые слова: мониторинг информационной безопасности, сетевые объекты, регистр сдвига.

Введение

Мониторинг информационной безопасности (далее - ИБ) сложных систем, в том числе имеющих структуру сети и относящихся к критической информационной инфраструктуре Российской Федерации, зарекомендовал себя как эффективный инструмент обеспечения их устойчивого функционирования. При этом при разработке критериев, используемых для оценки безопасности состояния сложной системы, как правило, используются знания о характерных особенностях внешнего и внутреннего поведения этой системы. В качестве, примеров таких особенностей можно привести запреты выходных последовательностей специального вида, построенных для автоматных моделей сетевых объектов, входящих в сложные системы, а также особенности функционирования указанных моделей и алгебраических структур, ассоциированных с ними. Ранее в работах Калашникова А.О., Мельникова С.Ю. и автора (см. [1-5]) в качестве механизмов для выявления особенностей внешнего поведения объектов мониторинга были предложены способы построения и использования гомоморфизмов автоматов, экспериментов с автоматами, а также отношений специального вида для автоматных и групповых моделей сложных систем, включая ассоциированные с ними комбинаторные объекты (определяемые на графах и мультиграфах состояний соответствующих автоматов). При этом для рассматриваемых автоматных моделей из класса недвоичных регистров сдвига и их обобщений, в том числе, для редуцированных графов Де Брейна, удалось предложить автоматные модели сетевых объектов, обладающие необходимыми свойствами для обеспечения целей мониторинга ИБ указанных объектов. В данной работе, на основе конструкции подстановок, определенных на смежных классах абелевой группы составного порядка по ее подгруппам (см. [6]), предложен ряд новых классов средств и механизмов мониторинга ИБ, которые позволяют реализовать более широкий спектр критериев оценки уровня защищённости сетевых объектов.

1 Основные понятия и определения

1.1 Обобщенный регулярный неавтономный регистр сдвига, действующий в абелевой группе

Автоматные модели мониторинга ИБ сетевых объектов будем рассматривать в рамках двух базовых сценариев: статического и динамического. При статическом сценарии будем предполагать, что набор параметров мониторинга фиксирован в соответствии с условиями функционирования объекта контроля, которые не могут быть изменены на протяжении всего периода его использования. Поэтому вариативность параметров автоматных моделей для статического сценария мониторинга ИБ ограничена выбором конкретных реализаций средств и механизмов контроля за состоянием защищенности объектов мониторинга из фиксированного классов таких средств и механизмов. В отличие от статического динамический сценарий допускает возможность расширения или сужения спектра средств и механизмов мониторинга сетевых объектов в зависимости от текущего состояния защищенности контролируемой сети и ее элементов. Данный подход к выбору средств и механизмов мониторинга ИБ сетевых объектов применительно к автоматным моделям, которые рассматриваются ниже, предусматривает необходимость обеспечения их соответствия достаточно широкому набору требований, соответствие которым было установлено для моделей регистрового типа, рассмотренным ранее в работах [1-5]. Поэтому в целях решения задачи, во-первых, построения новых автоматных моделей объектов мониторинга, обладающих положительными свойствами уже известных моделей, и, во-вторых, нахождения новых критериев для оценки безопасности состояния контролируемых объектов, применение которых совместно с новыми автоматными моделями окажется эффективным.

Определим базовое для последующего изложения понятие обобщенного неавтономным регистра сдвига, действующего в абелевой группе. Рассмотрим конечную абелеву группу G, которая имеет порядок $nm, n > 1, m > 1$, с операцией $+$ и нейтральным элементом 0, которая имеет подгруппы M и N порядков m и n соответственно (полагаем, что m и n - натуральные числа). Зафиксируем два множества: $p = \{p(1), \dots, p(n)\}$ - представителей смежных классов группы G по подгруппе M, а также $q = \{q(1), \dots, q(m)\}$ - представителей смежных классов группы G по подгруппе N. Пусть $\pi: p \longrightarrow N$ – некоторое биективное отображение множества p на группу N, $\varphi = (\varphi_1, \varphi_2, \dots, \varphi_n)$ – фиксированный набор биективных отображений подгруппы M на множество q, $\varphi_s: M \longrightarrow q, s = 1,2, \dots, n$, и, кроме того, $H = \{\chi_x | x \in X\}$ - некоторое подмножество симметрической группы $S(q)$ подстановок, действующих на множестве q и проиндексированных элементами некоторого непустого множества X.

Обобщенным (регулярным) неавтономным регистром сдвига (ОРС), действующим в группе G, назовем автомат $R(G) = (X, G, Y, h_{(\pi,\varphi)}(g, x), f_{(\pi,\varphi)}(g, x))$, у которого функция переходов $h_{(\pi,\varphi)}(g, x)$ и функция выходов $f_{(\pi,\varphi)}(g, x)$ для состояния $g = g + p(s)$, где $g_M \in M$, и входного символа $x \in X$ определены следующим образом:

$$h_{(\pi,\varphi)}(g, x) = h_{(\pi,\varphi)}(g_M + p(s), x) = (p(s))^{\pi} + (g_M^{\varphi_s})^{\chi_x},$$

$f_{(\pi,\varphi)}(g, x) = f_{(\pi,\varphi)}(g_M + p(s), x)$ - некоторое инъективное отображение группы G в множество выходных символов Y для каждого фиксированного $x \in X$.

В некоторых случаях функция выходов $f_{(\pi,\varphi)}(g, x) = f_{(\pi,\varphi)}(g_M + p(s), x)$ может представлять собой проекцию группы G на подгруппу M, продолженную на группу, изоморфную группе M. К такому случаю относится, например, ситуация, когда ОСР представляет собой автономный линейный регистр сдвига длины t над конечным полем P с унитарным характеристическим многочленом степени длины t, реализующий линейную рекуррентную последовательность с унитарным характеристическим многочленом степени t (см. [7]). При этом группа G является t -мерным векторным пространством над полем P, подгруппа M состоит из нулевого вектора и всех векторов, у которых отлична от нуля только первая координата, а все остальные равны нулю, подгруппа N является $(t-1)$-мерным пространством, состоящим из векторов с нулевой первой координатой, отображение π задает сдвиг информации по накопителю и, как правило, является тождественным, набор отображений φ определяет закон рекурсии и подстановка χ_x является тождественной для каждого $x \in X$.

Замечание 1. Регулярность автомата $R(G)$ следует (см. [6]) из биективности преобразования $\rho(\pi, \varphi)$ группы G, действие которого определяется равенством

$$g^{\rho(\pi,\varphi)} = (g_M + p(s))^{\rho(\pi,\varphi)} = (p(s))^{\pi} + g_M^{\varphi_s}.$$

Регулярность автоматной модели средства мониторинга является существенным полезным при эксплуатации свойством, поскольку используемый автомат всегда можно установить в исходное состояние путем подачи на вход подходящей установочной последовательности. В том числе по этой причине в работах [1-5] рассматривались регулярные регистры сдвига, действующие в конечных абелевых группах (см. также пояснение, приведенное в работе [6]), поэтому в рамках данной работы рассматриваются вопросы о теоретико-групповых и комбинаторных свойствах ОРС, который также является регулярным.

Использование гомоморфизмов ОРС, действующих в кольцах вычетов по простому модулю, позволило установить ряд новых свойств регистра сдвига с переносом (см., например, [8]), представляющих интерес для разработки критериев мониторинга их состояния, а также предложить ряд обобщений этого класса регистров сдвига с использованием колец, заданных на области их действия (см. [4]).

Для описания свойств группы $\Gamma_{R(G)}$ автомата $R(G)$ введем обозначения: $\Pi_{M,N}(p)$ – множество всех биективных отображение $\pi: p \longrightarrow N$ множества p на группу N, $\Phi_{M,N}(q)$ - множество всех наборов биективных отображений $\varphi = (\varphi_1, \varphi_2, \dots, \varphi_n)$ подгруппы M на множество q, $\overline{H} =< H >$ - группа, порожденная множеством H.

Замечание 2. Группа $\Gamma_{R(G)}$ автомата $R(G)$ содержит группу $\overline{H}_{\rho} = \rho(\pi, \varphi)^{-1} \overline{H} \rho(\pi, \varphi)$.

Универсальным (регулярным) регистром сдвига (УРС) $\tilde{R}(G)$, действующим в группе G, назовем семейство всех автоматов $R(G) = (X, G, Y, h_{(\pi,\varphi)}(g, x), f_{(\pi,\varphi)}(g, x))$, при задании которых используются все различные множества представителей p_j и q_j смежных классов группы G по ее подгруппам M и N, а также произвольные отображения $\pi \in \Pi_{M,N}(p_j)$ и $\varphi \in \Phi_{M,N}(q_j)$. Выделим в $\tilde{R}(G)$ подсемейство $\tilde{R}(G, \pi)$ ОРС, действующих в группе G, с фиксированными множеством $p = \{p(1), \dots, p(n)\}$ - представителей смежных классов группы G по подгруппе M, и отображением π,

которое назовем семейством ОРС с фиксированным сдвигом (СОРС). Отметим, что при определении УРС $\tilde{R}(G)$ предполагается, что подгруппы M и N порядков m и n, а также множество X являются фиксированными.

Отметим, что конструкции УРС и СОРС могут рассматриваться как общее описание автоматных моделей регистрового типа при их применении для решения задач статического сценария мониторинга ИБ сетевых объектов. Поэтому для применения ОРС в условиях динамического сценария мониторинга целесообразно расширить круг рассматриваемых объектов.

Рассмотрим семейство конечных абелевых групп $G_1, G_2, \dots, G_k$, каждая из которых определена на множестве $\Omega_N, |\Omega_N| = N$, причем для каждого $i \in \{1, \dots, k\}$ группа G_i порядка $N = n_i m_i, n_i > 1, m_i > 1$, имеет операцию $+_i$ с нейтральным элементом 0_i, а также содержит подгруппы M_i и N_i порядков m_i и n_i соответственно (как и ранее, m_i и n_i - натуральные числа),. Далее для каждого $i \in \{1, \dots, k\}$ обозначим множества $p_i = \{p_i(1), \dots, p_i(n_i)\}$ - представителей смежных классов группы G_i по подгруппе M_i, и $q_i = \{q_i(1), \dots, q_i(m_i)\}$ - представителей смежных классов группы G_i по подгруппе N_i. Пусть $\pi_i(p_i): p_i \longrightarrow N_i$ – некоторое биективное отображение для фиксированного множества p_i на группу N_i, $\varphi_i(q_i) = (\varphi_{i,1}, \varphi_{i,2}, \dots, \varphi_{i,n})$ – фиксированный набор биективных отображений подгруппы M_i на фиксированное множество q_i, $\varphi_{i,s}: M_i \longrightarrow q_i, s = 1,2, \dots, n_i$, и, кроме того, $H^{(i)} = \{\chi_x^{(i)} | x \in X_i\}$ - некоторое подмножество симметрической группы $S(q_i)$ подстановок, действующих на множестве q_i и проиндексированных элементами непустого множества X_i.

Групповым обобщенным регистром сдвига (ГРС) $\tilde{R}(G_1, G_2, \dots, G_k)$, действующим на множестве составного порядка Ω_N, назовем семейство всех УРС $\tilde{R}(G_i)$, где $i \in \{1, \dots, k\}$.

Замечание 3. Определение ГРС допускает возможность совпадения отдельных групп $G_1, G_2, \dots, G_k$ между собой, причем соответствующие подгруппы M_i и N_i, а также множества X_i, для $i \in \{1, \dots, k\}$, могут не совпадать для различных значений индексов. Поэтому в случае использования при задании ГРС упорядоченного набора различных групп, определенных на множестве Ω_N, будем использовать термин упорядоченный групповым обобщенный регистр сдвига (УГРС), действующим на множестве составного порядка Ω_N.

Конструкция ГРС, действующего на множестве составного порядка, предназначена, прежде всего, для создания условий интеграции информации, получаемой от средств мониторинга о состоянии различных, но однородных по своей структуре и базовым свойствам сетевых объектов. В частности, в качестве такого объекта мониторинга может рассматриваться сеть, состоящая из $N = nm$ элементов, состоянием которой является текущая конфигурация активных и пассивных элементов, изменение которой осуществляется в соответствии с их переключением по правилу, заданному ОРС, действующему в абелевой группе порядка N. Следует также отметить, что в рамках конструкции ГРС можно объединить регистры сдвига с неравномерным или даже обратным движением информации по накопителю.

Использование алгебраических структур, например, группы или кольца позволяет в ряде случаев упрощать задание и исследование свойств ОРС, действующих в абелевой группе (см., например, [6]). Однако последний приведенный пример показывает, что целесообразно предложить более общую по сравнению с ГСР комбинаторную конструкцию, в которой для задания подстановок на множестве составного порядка не используются алгебраические структуры, но при этом сохраняла бы основные черты регистра сдвига. Ниже приводится пример такой конструкции.

Свободным (регулярным) регистром сдвига (СРС) $\Re(\Omega_N)$, действующим на конечном множестве Ω_N составного порядка, $N = n_i m_i, n_i > 1, m_i > 1, \quad i \in \{1, \dots, l\}$, назовем семейство всех автоматов $R(\Omega_N, \gamma_i) = (X, \Omega_N, Y, h_{(\pi,\varphi,\gamma_i)}(c, x), f_{(\pi,\varphi,\gamma_i)}(c, x))$, у которых функция переходов определена по правилу: если $\Omega_N = A_i \times B_i$ – прямое произведение некоторых подмножеств A_i и B_i множества Ω_N, причем $|A_i| = n_i, |B_i| = m_i$, и $c = (a, b) \in \Omega_N, a \in A_i = \{a_1, a_2, \dots, a_{n_i}\}, b \in B_i = \{b_1, b_2, \dots, b_{n_i}\}$, для которых определены наборы $\bar{\pi}(i) = \left(\pi_{a_1}, \pi_{a_2}, \dots, \pi_{a_{m_i}}\right), \bar{\varphi}(i) = \left(\varphi_{b_1}, \varphi_{b_2}, \dots, \varphi_{b_{n_i}}\right)$ подстановок подмножеств B_i и A_i соответственно, и подстановка γ_i множества Ω_N, которая устанавливает взаимно однозначное соответствие между двумя представлениями множества Ω_N: $\Omega_N = A_i \times B_i$ и $\Omega_N = B_i \times A_i$, χ_x - некоторая подстановка из подмножества H группы $S(A_i)$, то

$$h_{(\pi,\varphi,\gamma_i)}(\mathrm{c}, x) = h_{(\pi,\varphi,\gamma_i)}((a, b), x) = ((b^{\pi_a}, (a^{\varphi_b})^{\chi_x}))^{\gamma_i},$$

$f_{(\pi,\varphi,\gamma_i)}(c, x) = f_{(\pi,\varphi,\gamma_i)}((a, b), x)$ - инъективное отображение группы G в множество выходных символов Y для каждого фиксированного $x \in X$.

В состав СРС входят все регистры $R(\Omega_N, \gamma_i)$, определенные для различных представлений множества Ω_N в виде прямого произведения двух подмножеств A_i и B_i множества Ω_N. Подстановки γ_i множества Ω_N, которые устанавливают соответствие между двумя представлениями в виде прямого произведения подмножеств множества Ω_N, вообще говоря, могут различаться для одних и тех же подмножеств A_i и B_i. Отметим, что пересечение подмножеств A_i и B_i может быть непустым, как и подгрупп M и N из определения ОРС, действующего в абелевой группе. В случае ОРС, действующего в абелевой группе G, функцию подстановок γ_i, которые фигурируют в определении СРС, «неявно» выполняет операция в этой группе. Поэтому при выделении подклассов автоматов, входящих в СРС, действующий на конечном множестве составного порядка, может оказаться удобным использование алгебраических структур, заданных на этом множестве.

Замечание 3. Регулярность автомата $R(\Omega_N, \gamma_i)$ следует из биективности преобразования $\Psi_{\overline{\pi}(i),\overline{\varphi}(i),\gamma_i}$ множества Ω_N, действие которого определено для элемента $c = (a, b) \in \Omega_N$ равенством

$$c\Psi_{\overline{\pi}(i),\overline{\varphi}(i),\gamma_i} = (a, b)\Psi_{\overline{\pi}(i),\overline{\varphi}(i),\gamma_i} = (b^{\pi_a}, a^{\varphi_b})^{\gamma_i}.$$

1.2 Механизмы мониторинга информационной безопасности и их параметры

В данном разделе перечислены основные механизмы и параметры средств мониторинга ИБ, автоматные модели которых описаны в п.1.1, и, тем самым, описан круг задач, рассматриваемых в данной работе:

1) Изучение свойств мультиграфов состояний автоматных моделей сетевых объектов

Для семейства конечных автоматов $A_i = (X_i, S_i, Y_i, h_i, f_i)$, $i \in \{1, N\}$, обладающих свойством: функция выходов f_i является инъективным отображением $f_i(x): S_i \to Y_i$, при каждом фиксированном $x \in X_i$ для всех $i \in \{1, N\}$ назовем l-недоступной k-грамму $(y_{j_1}, \dots, y_{j_k})$ l-недоступной для состояний $(s_{j_1}, \dots, s_{j_k})$, если для любых $x_1^i, \dots x_l^i$, $i \in \{1, N\}$, кортеж, состоящий из k выходных символов автоматов $A_{j_1}, \dots, A_{j_k}$ вида $f_{j_i}(\bar{h}_{j_i}(s_{j_i}, x_1^i, \dots, x_{l-1}^i), x_l^i)$, $i = 1, \dots, k$, не совпадает с $(y_{j_1}, \dots, y_{j_k})$.

При этом основными параметрами, характеризующими эффективность данного метода контроля, являются значения l и k. В качестве инструмента для их оценивания используется ориентированный граф $\Gamma_i^{[k]}$, построенный для каждого автоматов A_i, $i \in \{1, N\}$. Вершинами этого графа являются кортежи, состоящие из k попарно различных состояний автоматов A_i, а из вершины $(s_1, s_2, \dots, s_k)$ в вершину $(t_1, t_2, \dots, t_k)$ заходит дуга, если найдется входной символ $x \in X_i$ со свойством для каждого $j \in \{1, k\}$ и $s_j = (s_{1,j}, \dots, s_{k,j})$, $t_j = (s_{2,j}, \dots, s_{k,j}, h_i(s_{1,j}, x))$. Оценка диаметра $\partial(\Gamma_i^{[k]})$ графа $\Gamma_i^{[k]}$ позволяет определить максимальные значения параметра l и (или) описать множества заведомо недостижимых k-грамм.

Инъективность отображения $f_i(x): S_i \to Y_i$, при каждом фиксированном $x \in X_i$ позволяет решать одновременно задачу контроля l-недоступности k-грамм и для последовательностей состояний, и выходных последовательностей автоматных моделей сетевых объектов, поэтому функции выходов всех автоматы, определенных в п 1.1, обладают этим свойством.

2) Использование групп автоматных моделей сетевых объектов

Исследование групп Γ_A автоматных моделей A сетевых объектов позволяет, с одной стороны, указать верхние оценки параметра k, для которых значение диаметра $\partial(\Gamma_A^{[k]})$ заведомо бесконечно (если группа автомата не является k -транзитивной). С другой стороны, как отмечено в [9], информация о строении группы автомата и, в частности, ее транзитивности, примитивности и кратной транзитивности позволяет установить наличие угроз проведения атак на автомат, которые используют подмену средств мониторинга с помощью их гомоморфных образов.

3) Эквивалентность автоматных моделей сетевых объектов

Использование эквивалентных автоматных моделей мониторинга ИБ, выбираемых из достаточно представительного класса, является одним из способов противодействия атакам, указанным выше. Поэтому изучение вопросов эквивалентности в классах автоматов, являющихся разными вариантами обобщенного (регулярного) неавтономного регистра сдвига, действующего в абелевой группе, включая оценку числа классов эквивалентных автоматов, описание множества автоматов из данного класса, эквивалентных данному ОРС, построение внутренне изоморфных (подобных в терминологии групп подстановок) представителей классов УСР, ГСР, СРС, оценку вероятности эквивалентности двух ОРС, выбираемых из заданного класса в соответствии с определенной вероятностной схемой, представляет значительный интерес. В этот круг задач следует также включить выстраивание иерархических структур подклассов УСР, ГСР, СРС, элементы которых могут применяться на различных этапах статического или динамического сценариев мониторинга ИБ сетевых объектов.

4) Особенности строения графа автоматной модели

Граф автоматной модели A является частным случаем мультиграфа $\partial(\Gamma_A^{[k]})$ при $k = 1$. Однако его отдельные свойства, в частности, большое количество коротких (и даже единичных) циклов является очевидным недостатком автоматной модели, которого нужно избегать или иметь точный прогноз попадания на короткий цикл. Ранее вопросы исследования коротких циклов для редуцированных графов Де Брейна, близких по структуре к графам ОРС, рассматривался в [2]. Отметим, что регулярность рассматриваемых в данной работе автоматов позволяет не учитывать угрозы попадания на «длинный» подход к циклу. Кроме того, вопрос о связности и сильной связности автоматной модели может быть решен путем определения условий транзитивности соответствующей группы.

5) Периодические свойства автоматной модели

Данное направление представляет интерес при организации контроля за наследованием последовательностями состояний и выходных символов автоматных моделей периодических свойств их входных последовательностей

6) Разработка и оценка длины диагностических и установочных последовательностей, а также диагностических и контрольных тестов для автоматных моделей

Данное направление является классическим при синтезе автоматов и было применено в работе [4] при решении задач оценки качества контроля ИБ автоматами из класса, близко связанного с ОРС. Кроме того, данная информация позволяет получать дополнительные сведения об уровне защищенности объектов и средств мониторинга, а также разрабатывать и применять действенные меры по выводу из угрожающих ситуаций объектов мониторинга.

2 Основные результаты

2.1 Свойства групп и диаметров мультиграфов автоматов из классов УСР, СОРС, ГРС, СРС.

Утверждение 1. 1) если группа G не является прямой суммой своих подгрупп M и N, и при этом множество H действует транзитивно на множестве q, то группа $\Gamma_{R(G)}$ автомата $R(G)$ действует транзитивно на группе G;

2) если группа G является прямой суммой своих подгрупп M и N, то существуют такие множества p и q, отображения (τ, φ) и множество H, что группа $\Gamma_{R(G)}$ автомата $R(G)$ интранзитивна на группе G.

Следствие 1. В условиях п. 1 утверждения 1 группа любого автомата, принадлежащего УСР или СОРС, действующих в одной и той же абелевой группе, транзитивна.

Следствие 2. В условиях утверждения 1 любой автомат, принадлежащий УСР или СОРС, действующих в одной и той же абелевой группе, является сильно связным.

Всюду далее будем считать, что группа $\Gamma_{R(G)}$ автомата $R(G)$ действует транзитивно на группе G.

Замечание 4. Для автоматов, принадлежащих семействам ГРС и СРС, могут быть сформулировано аналогичное условия транзитивности их группы и сильной связности с поправкой на область действия подстановок, индексированных входными символами.

Достаточные условия конечности диаметра $\partial(\Gamma_{R(G)}^{[k]})$ для $k \leq 4$ содержит

Лемма 2. Если $k \leq 4$, множество H действует k-транзитивно на множестве q, $m = |q| \geq 3k$, все отображения $\varphi_s: M \longrightarrow q, s = 1,2,\dots,n$, различны, и подстановка $\varphi_s \varphi_{s'}^{-1}$ не имеет циклов длиною меньше 4 для всех $s \neq s'$, то группа $\Gamma_{R(G)}$ автомата $R(G)$ действует k-транзитивно на группе G.

Условия максимальности значений параметра k, при которых диаметр $\partial(\Gamma_{R(G)}^{[k]})$ является конечным позволяет получить

Утверждение 3. Если $n > 2m$ и множество H действует дважды транзитивно на множестве q, то группа $\Gamma_{R(G)}$ автомата $R(G)$ действует трижды примитивно на группе G.

Следствием из утверждения 3 является

Теорема 4. Если $n > 2m$, число nm не является степенью число 2 и множество H действует дважды транзитивно на множестве q, то группа $\Gamma_{R(G)}$ автомата $R(G)$ содержит знакопеременную группу $A(G)$ подстановок группы G.

Следствие 5. В условиях теоремы 4 группа любого автомата, принадлежащего УСР или СОРС, действующих в одной и той же абелевой группе, содержит знакопеременную группу $A(G)$.

В отдельных случаях удобно применять следующий результат

Теорема 6. Если $m > 4$ и множество H – группа, причем группа, порожденная группами $\overline{H}_\rho$ и H, содержит знакопеременную группу $A(q)$, то группа $\Gamma_{R(G)}$ автомата $R(G)$ содержит знакопеременную группу $A(G)$ подстановок группы G.

Конструкция ОРС, действующего в группе G позволяет более гибко по сравнению с классическими регистрами сдвига использовать свойства ее подгрупп и разбиения на классы по этим подгруппам, что упрощает, в частности, применение при изучении групп этих автоматов конструкции свободной связки групп подстановок (см. [9]) и делать акцент на свойствах групп подстановок малых степеней - $\overline{H}_\rho$ и $< H >$, которые сравнительно просто обеспечить.

Замечание 5. Для автоматов, принадлежащий УСР или СОРС и удовлетворяющих условиям теорем 4 и 6, диаметр $\partial(\Gamma_{R(G)}^{[k]})$ графа $\Gamma_{R(G)}^{[k]}$ является конечным для всех k, удовлетворяющих неравенству $1 \leq k \leq nm - 2$.

Для автоматов, принадлежащих семействам ГРС и СРС, могут быть сформулировано аналогичное условия конечности диаметров их мультиграфов с учетом областей действия подстановок, индексированных входными символами.

Конструкция ГРС позволяет более гибко по сравнению с классическими регистрами сдвига использовать подходящие подгруппы при задании ОРС и упрощать реализацию накладываемых на параметры автоматов условий, что подтверждает

Теорема 7. Если группа M содержит группу N , группа $\overline{H}_\rho$ действует примитивно на множестве q, и хотя бы одна подстановка $\varphi_s\varphi_{s'}^{-1}$ для $s, s' \in \{1,2,\dots,n\}$ является транспозицией, то группа $\Gamma_{R(G)}$ автомата $R(G)$ совпадает с симметрической группой $S(G)$ подстановок группы G.

При использовании каскадов (сетей последовательно включенных) ОРС полезно учитывать следующее свойство.

Утверждение 8. Если $m > n, n|m$, то для любых $N-$грамм $(s_1, s_2, \dots, s_N)$ и $(t_1, t_2, \dots, t_N)$ элементов множества составного порядка Ω_N найдутся такие три ОРС $R(G_i), i = 1,2,3$, принадлежащие ГРС, действующему на этом множестве, что для соответствующих этим ОРС подстановок $\rho_i(\pi_i, \varphi^{(i)})$, $i = 1,2,3$, выполнены равенства

$$t_j = s_j\rho_1(\pi_1, \varphi^{(1)})\rho_2(\pi_2, \varphi^{(2)})\rho_i(\pi_3, \varphi^{(3)}),\ j \in \{1,2,\dots,N\}.$$

Утверждение 9. В условиях теорем 4, 6 и 7 количество состояний неизоморфного гомоморфного образа соответствующего автомата не превосходит двух.

Последнее утверждение позволяет сделать вывод о том, что потенциальные атаки, связанные с попыткой подменить сетевой объект путем его «упрощения», малой эффективны в отношении ОРС, удовлетворяющих условиям перечисленных теорем.

Замечание 6. Свойства групп автоматов из класса СРС, не входящих в класс ГРС, не приведены из-за громоздкости формулировок.

2.2 Вопросы эквивалентности в автоматах из классов УСР, СОРС, ГРС, СРС.

Основные свойства эквивалентности в автомата, принадлежащих УРС, действующего в абелевой группе G, устанавливает

Утверждение 10. 1) каждый автомат $R(G) \in \tilde{R}(G)$ является минимальным, причем его степень различимости $\delta(R(G))$ равна 1;

2) для любого автомата $R(G) \in \tilde{R}(G, \pi)$ существуют $n!$ эквивалентных (внутренне изоморфных) ему автоматов $R'(G) \in \tilde{R}(G)$, при этом в самом классе $\tilde{R}(G, \pi)$ не существует отличных от $R(G)$ автоматов, внутренне изоморфных ему.

Следствие 11. 1) число классов эквивалентных автоматов в множестве $\tilde{R}(G)$ не превышает величины $m^{n-1}(n^{m-1}m!)(m!)^n$;

2) класс СОРС $\tilde{R}(G, \pi)$ является исключительным;

3) любой ОРС, принадлежащий классу $\tilde{R}(G, \pi)$ является распознаваемым в этом классе.

Основные свойства эквивалентности в автомата, принадлежащих ГРС и СРС, действующих на множестве Ω_N составного порядка, устанавливает

Утверждение 12. 1) каждый автомат A, принадлежащий ГРС и СРС, действующих множестве составного порядка, является минимальным, причем его степень различимости $\delta(A)$ равна 1;

2) два автомата $R(G_i), R'(G_j) \in \tilde{R}(G_1, G_2, \dots, G_k)$ не эквивалентны, если $G_i \neq G_j$;

3) два автомата $A_1, A_2 \in \Re(\Omega_N)$, не эквивалентны, если не совпадают пары подмножеств $\{A_1, B_1\}$ и $\{A_2, B_2\}$, используемые в определении этих автоматов;

4) память любого автомата, принадлежащего ГРС или СРС, равна 1.

Таким образом, решены основные принципиальные вопросы, касающиеся эквивалентности автоматов из рассматриваемых классов, что открывает возможность изучения их периодических свойств этих автоматов и построения экспериментов с этими автоматами. Приведенное в п. 4)

утверждения 12 значение памяти ОРС позволяет строить короткие контрольные тесты для проверки корректности функционирования этих автоматов.

2.3 Периодичность и наследственность в автоматах из классов УСР, ГРС, СРС.

Из свойств функций переходов и выходов ОРС, определенных в разделе 1.1, и результатов раздела 2.2 следует важное при использовании периодических последовательностей для тестирования работоспособности сетевого объекта с помощью его автоматной модели.

Утверждение 13. 1) если у автомата A, который принадлежит одному из семейств УСР, ГСР, СРС, подстановки, принадлежащие множеству H, которое используется при определении данного автомата, попарно различны, то такой автомат является внутренне наследственным;

2) в условиях п. 1) автомат A является внешне наследственным;

3) в условиях п. 1) подход входной периодической последовательности не превышает подходов соответствующих последовательности состояний и выходной последовательности автомата A;

4) в условиях п. 1) периоды последовательности состояний и выходной последовательности автомата A кратны периоду соответствующей входной периодической последовательности.

Полученные результаты позволяют обосновать эффективность использования периодических входных последовательностей для тестирования текущего состояния объекта мониторинга. При этом из п. 3) утверждения 13 можно сделать вывод о том, что такие тестовые последовательности не всегда должны выбираться чисто периодическими, что дает возможность расширить спектр механизмов мониторинга, например, за счет случайного выбора подхода тестовой последовательности.

2.4 Эксперименты с автоматами из классов УСР, ГРС, СРС.

В разделе 2.2 установлено, что каждый автомат, принадлежащий одному из рассматриваемых классов, является минимальным. Тем самым выполнено исходное условие построения экспериментов по распознаванию состояний ОРС R, действующего на множестве составного порядка nm (принадлежащего любому из классов УСР, ГРС, СРС), и, в частности, ОРС всегда можно установить в некоторое известное состояние, и если группы автомата транзитивна найти его начальное состояние. Однако в случае ОРС задачу построения экспериментов по распознаванию состояний можно рассмотреть в более общей постановке, а именно, когда известны входная последовательность $x(1), x(2), \dots, x(t)$ и только отдельные фрагменты выходной последовательности $y(t_1), \dots, y(t_d)$, где $t_1 < t_2 < \dots < t_d$, $t_i, i \in \{1, \dots, d\}$, – номера тактов. Условия существования простых диагностических экспериментов ОРС, а также оценки длины диагностических и установочных экспериментов по распознаванию состояний ОРС содержит

Утверждение 14. 1) если известен текущий выходной символ $y(t_i)$, $i \in \{1, \dots, d\}$, то текущее состояние ОРС R может быть определено путем частичного обращения функции выходов, действие которой ограничено на множестве состояний;

2) если группа Γ_R ОРС R транзитивна, то такой ОРС всегда может быть установлен в заданное состояние с помощью простого эксперимента длиною не более $nm - d + 1$;

3) если группа Γ_R ОРС R транзитивна, а также известны номер такта $t_i, i \in \{1, \dots, d\}$ и текущий выходной символ $y(t_i)$, то начальное состояние ОРС всегда может быть определено с помощью простого эксперимента, длина которого не превышает $d - 1$;

4) если группа Γ_R ОРС R дважды транзитивна, номера тактов t_i, t_j $t_i < t_j, i, j \in \{1, \dots, d\}$, а также выходной символ $y(t_j)$ известны, то начальное состояние ОРС всегда может быть определено с помощью простого эксперимента, длина которого не превышает $j - i + 1$.

Таким образом, для ОРС, независимо от класса которому он принадлежит, длина установочного эксперимента равна 1, а длина диагностического эксперимента не превышает в зависимости от свойств группы автомата номера такта самого позднего отклика.

В отношении задач тестирования неисправностей ОРС в их классической постановке отметим, что, исходя из общей теории распознавания неисправностей, построение диагностического и контрольного тестов возможно для ОРС, принадлежащего СОРС, при условии, что все рассматриваемые неисправности не выводят за пределы класса СОРС (см. следствие 11). Поэтому вопросы тестирования неисправностей ОРС в общем случае пока остаются открытыми. Вместе с тем, для конкретных видов атак, приводящих к нарушению функционирования ОРС, можно использовать специализированные методы их выявления и противодействия. В качестве примеров таких методов противодействия в данной работе предложен ряд процедур и приведены условия их эффективного применения, в том числе, для коротких тестов корректности функционирования ОРС, использующих малую величину его

памяти, контрольных периодических последовательностей, использующих свойства внешней и внутренней наследственности ОРС из рассматриваемых классов, а также мультиграфов состояний автоматов, опирающихся на теоретико-групповые свойства рассматриваемых автоматных моделей и их каскадных (последовательных) соединений.

Заключение

Приведенные выше результаты и предложенные механизмы мониторинга ИБ сетевых объектов показывают возможность эффективного использования автоматных моделей, построенных на базе обобщённых регистров сдвига в качестве основного направления дальнейших исследований эффективности использования таких автоматов представляется целесообразной проработка вопросов оптимального управления параметрами указанных объектов в интересах мониторинга защищенности критической инфраструктуры Российской Федерации.

Литература

1. *Калашников А.О., Максимовский А.Ю.* Использование специальных соотношений в автоматах для мониторинга информационной безопасности сетевых объектов //Информация и безопасность. 2019. Том 22. – № 1 (1). – С. 30-37.
2. *Максимовский А.Ю., Мельников С.Ю.* Спектральные и комбинаторные свойства редуцированных графов Де Брейна //Вопросы кибербезопасности. - 2018. – № 4 . – С. 70-76.
3. *Калашников А.О., Максимовский А.Ю.* Развитие автоматных моделей мониторинга информационной безопасности сетевых объектов //Информация и безопасность. 2019. Том 22. – № 4 (4). – С. 549-556.
4. *Максимовский А.Ю.* О двух классах автоматов над конечными кольцами, построенных на основе изоморфизма регистра сдвига с переносом и их применении для защиты информации //Вопросы кибербезопасности. - 2019. – № 1 (29). – С. 69-76.
5. *Калашников А.О., Бугайский К.А., Аникина Е.В*. Модели количественного оценивания компьютерных атак. Часть 1.//Информация и безопасность. 2019. Том 22. – № 4 (4). – С. 517-528.
6. *Максимовский А.Ю.* О групповых свойствах подстановок, определенных на смежных классах конечной абелевой группы по ее подгруппам //Математические вопросы криптографии. - 2016. – Т. 7 , № 1 (29). – С. 83-92.
7. *Гилл А.* Линейные последовательные машины. - М.: Мир, 1974. – 288с.
8. *Klapper A, Goresky M*. Feedback Shift Registers, 2-Adic Span, and Combiners with Memory // J.Cryptology, Vol. 10. 1992, № 2, P. 111-147.
9. *Максимовский А.Ю.*. О применении конструкции свободной связки групп подстановок для обеспечения киберустойчивости информационно-управляющих систем / Материалы 12-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD’2019, Москва) – М.: ИПУ РАН, 2019. – С.1049-1050.