Управление доступом к ресурсам ведомственных информационных систем на основе информационных профилей пользователей

Access control of information resources for departmental information systems based on information user profiles

Саенко / Saenko I.
Игорь Борисович
(ibsaen@mail.ru)
доктор технических наук, профессор.
ФГКВОУ ВО «Военная академия связи имени Маршала Советского Союза С. М. Буденного» МО РФ (ВАС им. С. М. Буденного),
профессор.
г. Санкт-Петербург

Кий / Kiy A.
Андрей Вячеславович
(kiyarmy@yandex.ru)
кандидат технических наук.
ВАС им. С. М. Буденного,
доцент кафедры автоматизированных систем специального назначения.
г. Санкт-Петербург

Ясинский / Yasinsky S.
Сергей Александрович
(yasinsky777@mail.ru)
доктор технических наук, доцент.
Филиал ФГУП «Ленинградское отделение центрального научно-исследовательского института связи» (ЛО ЦНИИС),
научный консультант.
г. Санкт-Петербург

Лыжинкин / Lyzhinkin K.
Константин Владимирович
(lkv@loniis.ru)
Филиал ФГУП ЛО ЦНИИС,
заместитель директора.
г. Санкт-Петербург

Ключевые слова: защита информации – information security, политика безопасности – security policy, контроль доступа – access control, информационный профиль – information profile.

В статье рассматривается проблема обеспечения безопасности информации в ведомственных информационных системах. Обосновывается необходимость применения в составе системы защиты информации механизмов, обеспечивающих контроль выполнения пользователями процедур обработки информации, определенных требованиями политики безопасности и основанных на применении профилей пользователей. Предложена методика построения профилей пользователей на основе цепей Маркова и методов кластерного анализа.

The paper considers a problem of information security in the departmental information systems. Need of an application as a part of the system of information security the mechanisms providing control of execution by users the procedures processing information determined by requirements of a trust relationships policy and based on application of user profiles is justified. The technique of creation of user profiles on the basis of the Markov chains and methods of cluster analysis is offered.

Введение

Обеспечение устойчивого и бесперебойного функционирования информационной, и в первую очередь критической, инфраструктуры Российской Федерации является одним из ключевых национальных интересов в информационной сфере [1]. В связи с этим в ведомственных информационных системах (ВИС) к обеспечению безопасности информационного процесса предъявляются особые требования, которые определяются уровнем конфиденциальности обрабатываемой информации и особенностями условий функционирования данных систем. По этой причине большое значение уделяется развитию, разработке и внедрению систем управления информацией и событиями безопасности [2], которые обеспечивают поддержание требуемого уровня базовой безопасности, установленного руководящими документами для каждого типа таких систем.

Уровень базовой безопасности достигается путем реализации минимального пакета защитных мер, известных как базовые защитные меры. Вследствие различий в процессах выбора защитных мер могут

4 2017.indd 119 12.12.2017 11:25:48

рассматриваться следующие два пути обеспечения уровня базовой безопасности [3]:

реализация защитных мер в соответствии с типом и характеристиками рассматриваемой системы;

реализация защитных мер в соответствии с базовой типовой моделью угроз безопасности информации, а также в зависимости от характеристик рассматриваемой системы.

В большинстве случаев для обеспечения требуемого уровня безопасности в ВИС применяется первый подход, основанный на классификации информационных систем по уровню защищенности. Однако статистика нарушений безопасности в таких системах показывает, что на практике для обеспечения безопасности информации требуются дополнительные защитные меры. Это связано с тем, что любая политика безопасности и реализующая ее система защиты работают только в случае, если их соблюдают пользователи системы.

В связи с этим возникает необходимость в проверке (контроле) выполнения процедур обеспечения безопасности в действиях пользователей, а также корректности (полномочности) использования предоставленных в доступ информационных ресурсов ВИС. Данная задача может быть решена применением интеллектуальных средств защиты информации, реализующих постоянный, осуществляемый в онлайн-режиме, контроль состояний системы на предмет соответствия некоторому набору эталонов, включающих множество допустимых значений наиболее существенных характеристик информационного процесса, образующих информационный профиль пользователя.

Механизм управления доступом к данным на основе информационных профилей пользователей

Анализ и использование информационных профилей пользователей представляется достаточно эффективным решением в области защиты от несанкционированного доступа к информации в ВИС. Под информационным профилем элемента ВИС при этом будем понимать структурированное формализованное описание существенной для защиты информации области в пространстве признаков состояний элемента либо информационных отношений между элементами ВИС, в которой отображается множество эквивалентных с точки зрения управления состояний или траекторий поведения элемента [4].

Анализ нарушений безопасности информации в ВИС показывает, что в большинстве случаев источником угроз безопасности информации является авторизованный пользователь системы. Это обуславливает актуальность подходов к защите информации в ВИС с использованием информационных профилей пользователей. В ВИС основными типами профилей субъектов являются образы процесса реализации пользователями нарушений безопасности информации, т.е. образы состояния создания и реализации угроз безопасности, а также образы безопасного функционирования ВИС.

Применение профилей (образов) безопасного функционирования ВИС в целях защиты от внутренних угроз безопасности является более предпочтительным, так как позволяет выявлять ранее неизвестные типы и сценарии реализации угроз несанкционированного доступа. В целях управления доступом к информационным ресурсам ВИС указанные профили должны отражать схемы использования информационных ресурсов пользователями в процессе выполнения множества функциональных задач, что позволит применять их в качестве дополнительного критерия при принятии решения о предоставлении того или иного вида доступа к информационным ресурсам.

Структура механизма управления доступом к данным на основе информационных профилей пользователей представлена на рис. 1.

Представленный механизм управления доступом состоит из следующих основных компонентов:

– компонент контроля соответствия таблице разграничения доступа на основе дискреционной и мандатной моделей управления доступом;

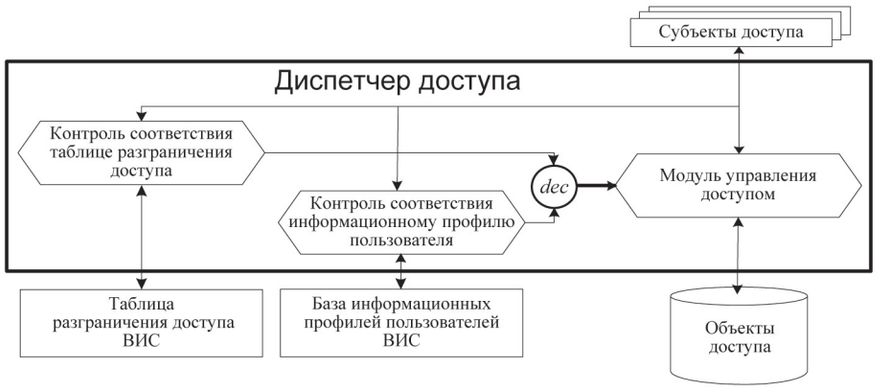

Рис. 1. Механизм управления доступом на основе информационных профилей пользователей

4-2017.indd 120 12.12.2017 11:25:48

– компонент контроля соответствия информационному профилю на основе сравнения данных о текущих событиях безопасности и характеристик элементов информационного профиля пользователя;

– компонент принятия решения о доступе (*dec*);

– модуль управления доступом.

Особенностью предложенного механизма является принятие решения о доступе не только на основе матрицы разграничения доступа, введенной администратором безопасности ВИС, но и на основе контроля событий безопасности, поступающих с уровня сбора и обработки данных. Контролируется соответствие событий безопасности эталонным значениям информационного профиля, определяемым на основе списка активных процессов пользователя. Тем самым обеспечивается динамика изменения прав доступа в процессе работы пользователя.

Описание и формирование профилей пользователей

Основу любой системы защиты информации от несанкционированного доступа в ВИС составляет подсистема управления доступом, ключевыми задачами которой являются предотвращение несанкционированного использования защищаемых ресурсов ВИС и предотвращение использования ресурсов неполномочным способом. Первая задача решается с помощью разграничения доступа в соответствии с принятой политикой безопасности и последующего контроля запрашиваемых видов доступа на предмет соответствия предоставленным полномочиям [5].

Задача контроля процедур безопасности использования информационных ресурсов в основном решается организационными мерами, которые предполагают описание правил использования информационных ресурсов и обеспечение их соблюдения. При этом важную роль играют дисциплина и уровень подготовки пользователей. Однако независимо от принятых организационных мер и полноты настроек системы разграничения доступа (СРД) невозможно избежать нарушений политики безопасности. Причинами этого могут быть ошибки при составлении частной модели угроз безопасности для конкретной ВИС, влияющие на выбор используемых методов и средств защиты, противоречивые правила доступа, ошибки администрирования, упрощение политики в процессе настройки СРД, ошибки пользователей, незнание или непонимание политики безопасности пользователями ВИС.

Примерами нарушения процедур безопасного использования предоставленных в доступ информационных ресурсов могут быть копирование информации из файлов, доступных для чтения, разделение файлов, модификация файлов при наличии прав доступа, попытки пользователей получить доступ к информационным ресурсам путем «изучения» ВИС, ознакомление с конфиденциальной информацией, не предназначенной пользователю, и др. В случае таких нарушений, как правило, отсутствует реакция средств защиты, так как перечисленные действия не нарушают в явном виде политику безопасности. В связи с этим возникает необходимость развития средств управления доступом, способных классифицировать в режиме реального времени легальные действия пользователей по степени опасности для ВИС и принимать на основании заранее определенного набора правил решение о доступе или ограничении полномочий пользователя.

В основе реализации таких механизмов могут быть использованы информационные профили пользователей, описывающие легитимный порядок использования информационных ресурсов ВИС в процессе их деятельности и обеспечивающие принятие решения о правомочности доступа к ресурсу на основе текущей активности пользователей. В связи с этим одним из направлений совершенствования системы защиты информации ВИС является разработка математического и методического аппарата описания и формирования указанных профилей.

С целью определения структуры информационного профиля пользователя и информативных признаков для его построения проведен анализ факторов, влияющих на особенности организации работы пользователей ВИС. К ним относятся: наличие конечного, четко обозначенного в обязанностях перечня функций, выполняемых пользователем; регламентация порядка выполнения указанных функций; цикличность процессов, реализуемых пользователем.

Кроме того, выполнение пользователем каждой функции и реализация соответствующих ей процессов предопределяет набор программ и порядок их использования. Каждая программа имеет функциональное назначение, в рамках которого обладает возможностями по доступу к информационным ресурсам ВИС. Следовательно, выполнение пользователем функциональной задачи можно представить в виде последовательности операций доступа к ресурсам с использованием необходимых программных средств:

$$ts_e = \left\langle (q_1, q_2, ..., q_a)_{ts_e}, PR_{ts_e} \right\rangle, \qquad (1)$$

где q_a – элемент последовательности операций доступа в процессе выполнения функциональной задачи ts_e; $PR_{ts_e} = \{pr_l\}$ – множество программных средств (программ), необходимых для выполнения функциональной задачи ts_e.

Таким образом, наиболее информативным признаком, отражающим действия пользователя при выполнении функциональной задачи, является событие доступа, представляющее собой комбинацию операции (типа) доступа и идентификатора информационного ресурса. Так как время в вычислительной среде дискретно, а действия пользователя имеют целенаправленный

4-2017.indd 121 12.12.2017 11:25:48

характер, то наблюдаемая последовательность событий доступа представляет собой случайный процесс с дискретными состояниями и дискретным временем, что позволяет использовать для описания деятельности пользователя аппарат Марковских цепей [6]. В связи с этим, учитывая (1), информационный профиль пользователя ip при выполнении функциональной задачи ts_e должен содержать элементы $ip^{ts_e} = \left\langle \Lambda^{ts_e}, PR^{ts_e} \right\rangle$, где: $\Lambda^{ts_e} = [\mathrm{N}^{ts_e}, \mathrm{K}^{ts_e}]$ – Марковская модель наблюдения событий доступа в процессе выполнения пользователем функциональной задачи ts_e; N^{ts_e} и K^{ts_e} – соответственно вектор начального распределения вероятностей событий доступа и матрица переходных вероятностей событий доступа в процессе выполнения функциональной задачи ts_e; $PR^{ts_e} = \{pr_l\}$ – множество программных средств, необходимых для выполнения задачи ts_e.

Выбор пользователем программ для выполнения той или иной функциональной задачи, порядок их активизации и использования осуществляется на основании содержания задачи, нормативных документов, определяющих порядок ее выполнения, состава и характеристик программного обеспечения. Из вышесказанного следует, что изменение списка активных программ на рабочей станции пользователя свидетельствует о переходе к выполнению очередной функциональной задачи. В связи с этим имеется возможность разбиения последовательности событий доступа на фрагменты деятельности пользователя (ФДП), каждый из которых соответствует выполнению некоторого непрерывного этапа функциональной задачи. Формирование ФДП начинается с появления события $q_a = (\tau_a, d_r)$ и заканчивается с появлением события $q_b = (\tau_{a+1}, d_s)$. Последовательность событий доступа, наблюдаемая в интервал времени $\tau_a \le \Delta t < \tau_{a+1}$, определяет содержание ФДП с идентификатором d_r.

Формирование информационного профиля u-го пользователя осуществляется путем разбиения множества $Q^u = \{Q_h\}$ ФДП на множество классов, каждый из которых содержит однородные в смысле близости переходных вероятностей событий доступа фрагменты, где $h = 1, H^u$ – h-й ФДП u-го пользователя. Для проведения классификации каждый фрагмент представляется матрицей вероятностей переходов W_h входящих в него событий доступа, имеющей следующий вид:

$$W_h = [w_{\chi\eta}] = \begin{bmatrix} w_{11}^h & w_{12}^h & \dots & w_{1J}^h \\ w_{21}^h & w_{22}^h & \dots & w_{2J}^h \\ \dots & \dots & \dots & \dots \\ w_{J1}^h & w_{J2}^h & \dots & w_{JJ}^h \end{bmatrix},$$

где $w_{\chi\eta}^h$ – вероятность наблюдения события доступа q_η после наблюдения события доступа q_χ в рамках h-го ФДП.

Представление матриц вероятностей переходов W_h в виде векторов V_h, характеризующих размещение точки в J-мерном пространстве, позволяет применить для выявления типовых схем использования информационных ресурсов методы кластерного анализа. В связи с тем, что компоненты вектора V_h однородны по своему физическому смыслу и одинаково важны с точки зрения решения вопроса об отнесении вектора V_h к тому или иному классу, в качестве меры близости векторов принято евклидово расстояние

$$\rho(V_a, V_b) = \rho_{ab} = \rho_{ba} = \sqrt{\sum_{\mu=1}^{J^2} (v_\mu^a - v_\mu^b)^2}, \qquad (2)$$

где $\rho(V_a, V_b) = \rho_{ab} = \rho_{ba}$ – расстояние между векторами V_a и V_b в евклидовом пространстве; v_μ^a – μ-й элемент вектора V_a; v_μ^b – μ-й элемент вектора V_b.

Проведенный анализ методов кластерного анализа показал, что иерархические методы позволяют не только внести структуру в данные, но и описать схемы использования информационных ресурсов с различной степенью детализации в зависимости от шага процедуры (уровня иерархии) на котором получен класс. В основе алгоритмов иерархического кластер-анализа лежит тот или иной критерий качества $\theta(\Phi^{(k)})$ разбиения, где k – количество классов, полученных в результате разбиения исходного множества. При этом обычно, если $k = 2$, то используются бинарные алгоритмы [7]. В этом случае $\theta(\Phi^1, \Phi^2)$ имеет смысл близости $\rho(\Phi^1, \Phi^2)$ между множествами Φ^1 и Φ^2.

Делимые бинарные алгоритмы строятся на принципе разделения множества $Q^u = \{Q_h\}$ ФДП на подмножества $\Phi_\beta^{(*)} = \{\Phi^1, \Phi^2\}$ такие, что $(\Phi^1, \Phi^2) = \arg\max_{\Phi^1 \cup \Phi^2 = \Phi} \rho(\Phi^1, \Phi^2)$, где (*) – вариант разделения исходного множества на два класса, полученный на β-ом шаге кластеризации.

На каждой итерации «родительский» класс разбивается на два подкласса до тех пор, пока не будет выполнено условие останова, либо пока каждый ФДП не образует отдельный класс. Для множества $Q^u = \{Q_h\}$ ФДП, входящих в «родительский» класс на β-ом шаге кластеризации, могут быть получены различные варианты разбиения на подклассы. В качестве критерия однородности класса $\Phi_\beta \subset \{V_h\}$ возьмем статистический разброс $\theta(\Phi_\beta)$ [7]:

$$\theta(\Phi_\beta) = \sum_{h=1}^{H^u} \left| \text{Ц}^k - V_h \right|,$$

где Ц^k – центр класса Φ^k; $\left|\text{Ц}^k - V_h\right|$ – «манхэттенское» расстояние (среднее разностей между координатами) между центром класса Φ^k и элементом класса V_h. В свою очередь центр класса Φ^k определяется в соответствии со следующим выражением [8]:

$$\text{Ц}^k = \frac{1}{|H_k|} \sum_{h=1}^{H_k} V_h, \qquad (3)$$

где H_k – количество элементов множества, отнесенных к классу Φ^k.

4-2017.indd 122 12.12.2017 11:25:49

Положим, что мерой близости между классами является приращение статистического разброса при объединении классов [9]

$$\rho(\Phi^1,\Phi^2)=\theta\left(\Phi^1\cup\Phi^2\right)-\theta\left(\Phi^1\right)-\theta\left(\Phi^2\right),\ \Phi^1\cap\Phi^2=\varnothing.$$

Тогда из множества вариантов разбиения на классы $\Phi_\beta^{(*)}$ необходимо выбрать наилучший вариант, соответствующий минимальному значению функционала качества разбиения, определяемый следующим выражением [9]:

$$\theta(\Phi^1,\Phi^2)^{(*)}=\arg\min_{\Phi^1\cup\Phi^2=Q} F\left(\Phi^1,\Phi^2\right),$$

где $F\left(\Phi^1,\Phi^2\right)=\theta\left(\Phi^1\right)+\theta\left(\Phi^2\right)$, где $\theta\left(\Phi^1\right)$ – статистический разброс класса Φ^1; $\theta\left(\Phi^2\right)$ – статистический разброс класса Φ^2; $F\left(\Phi^1,\Phi^2\right)$ – функционал качества разбиения множества Q ФДП на классы Φ^1 и Φ^2 в методе 2-средних.

Кластерный анализ решает задачу внесения структуры в данные. В связи с этим необходимо найти меру качества, которая показывает, насколько хорошо описание из k классов соответствует данным. Так как аналитическое выражение для оптимального разбиения отсутствует, то невозможно вывести точного решения для распределения данных. При этом можно получить приблизительное решение, близкое к оптимальному. В связи с тем, что на каждом шаге кластер-процедуры требуется определить возможность разбиения «родительского» класса на два, применяем следующий критерий останова $F_{\text{ост}}$ [10]:

$$F_{\text{ост}}=\frac{w[2]}{w[1]}>F_{\text{крит}}, \tag{4}$$

где $F_{\text{крит}}$ – критическое значение критерия останова; $w[2]$ – сумма квадратов внутрикластерных расстояний в случае распределения ФДП по двум классам; $w[1]$ – сумма квадратов внутрикластерных расстояний в случае одного класса. В свою очередь сумма квадратов внутрикластерных расстояний определяется в соответствии со следующим выражением [10]:

$$w[\mathrm{k}]=\sum_{k=1}^{K}\sum_{\substack{a,b\in\Phi^k\\ a\neq b}}^{H_k}\rho_{ab}^2,$$

где $k=\overline{1,K}$ – количество классов; H_k – количество ФДП, входящих в класс Φ^k; ρ_{ab}^2 – квадрат внутрикластерного расстояния между элементами класса Φ_k.

Гипотеза о существовании единого кластера однородных данных отвергается, если значение критерия $F_{\text{ост}}$ меньше, чем критическое значение $F_{\text{крит}}$. В свою очередь $F_{\text{крит}}$ определяется следующим выражением [10]:

$$F_{\text{крит}}=1-\frac{2}{H_p\times J^2}-z_{1-\alpha}\times\sqrt{\frac{2\times\left(1-8/\pi^2\times J^2\right)}{H_p\times J^2}},$$

где H_p – количество ФДП, подлежащих классификации; J – число признаков классификации; $z_{1-\alpha}$ – квантиль стандартного нормального распределения уровня $(1-\alpha)$; α – уровень значимости при проверке гипотезы.

Процедура классификации на каждом шаге заключается в нахождении наилучшего разбиения множества ФДП на классы $\Phi_\beta=\{\Phi^1,\Phi^2\}$, которое отвечает следующему условию:

$$\theta(\Phi_\beta)=\min\left(\theta\left(\Phi^1\right)+\theta\left(\Phi^2\right)\right),$$

где β – цикл кластер-процедуры.

Проверка обоснования разбиения “родительского” класса осуществляется путем проверки выполнения критерия (4). В случае подтверждения гипотезы о существовании во множестве ФДП двух классов осуществляется его разбиение методом 2-средних. Общую последовательность разбиений можно ограничить, отбросив разбиения с мало наполненными кластерами, начиная с некоторого допустимого (порогового) значения информативности $H^{\text{доп}}$.

Нулевая итерация заключается в выборе двух векторов, которые назначаются центрами кластеров. В рамках предлагаемой кластер-процедуры выбор начальных центров классов осуществляется по результатам предварительной разметки признакового пространства, что позволяет выбрать начальные центры классов, распределенные более равномерно в исходном множестве. Выбор начальных центров классов основан на предварительной (грубой) классификации ФДП на основании анализа геометрического различия графического представления законов распределения событий доступа, входящих в состав ФДП. С этой целью каждому ФДП Q_h ставится в соответствие величина ψ_h, характеризующая подобласть исходного множества, в которой расположен соответствующий ей вектор V_h:

$$\psi_h=\sum_{j=1}^{J}\left(\sum_{a=1}^{j}\left(\frac{1}{J}-u(q_a|Q_h)\right)\right),$$

где $u(q_a|Q_h)$ – относительная частота появления событий доступа q_a в составе ФДП Q_h. Из полученных для всех ФДП значений величины ψ_h находятся минимальное и максимальное значения $\psi^{\min}$ и $\psi^{\max}$ указанной величины. Отрезок $[\psi^{\min};\psi^{\max}]$ делится на два отрезка одинаковой длины. Формируется два $\psi^{\text{ц}}$ центра отрезков $\psi^{\text{ц}}=\{\psi^{\text{ц},1},\psi^{\text{ц},2}\}$, где $\psi^{\text{ц},k}$ – центр k-го отрезка. В качестве начального центра k-го класса выбирается такой ФДП, для которого справедливо:

$$\mathrm{len}(\psi_h,\psi^{\text{ц},k})=\min_{1\le h\le H}\mathrm{len}(\psi_h,\psi^{\text{ц},k}),$$

где $\mathrm{len}(\psi_h,\psi^{\text{ц},k})$ – расстояние от ψ_h до $\psi^{\text{ц},k}$.

Последующие итерации заключаются в отнесении каждого вектора, из числа оставшихся, к одному из

4-2017.indd 123 12.12.2017 11:25:50

двух классов по критерию минимума расстояния от центра класса. В качестве меры близости векторов используется евклидово расстояние (2). После отнесения каждого очередного ФДП к классу осуществляется пересчет координат центра $Ц_k^{(i)}$ класса k:

$$ц_{k\mu}^{(i)} = \frac{1}{H_k^{(i)}} \sum_{h=1}^{H_k^{(i)}} v_\mu^h, \ \mu = \overline{1, J^2}.$$

Процедура заканчивается, когда все вектора будут распределены по классам. Затем выбираются другие два вектора, которые назначаются центрами классов, и процедура кластеризации повторяется до выполнения условия останова. Множество полученных в каждом цикле кластер-процедуры классов в соответствии с количеством входящих в их состав элементов делится на подмножество информативных классов $\Phi_{\beta+}$, у которых $H_\beta \geq H^{доп}$, и подмножество неинформативных классов $\Phi_{\beta-}$, у которых $H_\beta < H^{доп}$. В отношении множества неинформативных классов проводится процедура восстановления, которая заключается в объединении множества $\Phi_{\beta-}$, полученных на β-ом цикле кластер-процедуры, невзвешенным центроидным методом с ближайшим информативным классом $\Phi_{(\beta+1)+}$, полученным на $(\beta+1)$-ом цикле. По окончании выполнения процедуры восстановления информативным классам присваивается идентификатор β, соответствующий номеру цикла кластер-процедуры. В результате кластер-процедуры будет получен вариант разбиения исходного множества ФДП u-го пользователя ВИС на иерархически упорядоченное множество кластеров $\Phi^u = \{\Phi_{g,\beta}\}$, $g = \overline{1, G_\beta}$, $\beta = \overline{1, Z^u}$, где $\Phi_{g,\beta} = \{Q_h\}$ – g-й класс ФДП, полученный на β-ом цикле кластер-процедуры. Каждому классу ставится в соответствие множество идентификаторов ФДП $D_g = \{d_r\}$, входящих в состав класса.

Каждый полученный класс ФДП является элементом иерархического информационного профиля пользователя ВИС, содержит однородные в смысле близости вероятностных характеристик элементы и представляет собой типовую устойчивую схему использования пользователем информационных ресурсов ВИС. В качестве эталона для каждого класса принимается матрица вероятностей переходов, соответствующая его центру тяжести (3). Формирование векторов начального распределения вероятностей событий доступа $C_{g,\beta} = [c_{g,\beta,i}]$ для каждого класса ФДП осуществляется в соответствии с выражением:

$$c_{g,\beta,i} = \frac{1}{H_{g,\beta}} \sum_{Q_h \in \Phi_{g,\beta}} \varphi(Q_h),$$

где $H_{g,\beta}$ – количество ФДП, входящих в состав класса $\Phi_{g,\beta}$; $\varphi(Q_h)$ – функция, определяемая следующим образом:

$$\varphi(Q_h) = \begin{cases} 1, \text{ при } q_1 = m_i | q_1 \in Q_h, \\ 0, \text{ в противном случае.} \end{cases}$$

В результате информационный профиль пользователя IP содержит элементы $ip_{g,\beta} = \langle \Lambda_{g,\beta}, D_{g,\beta} \rangle$, где $\Lambda_{g,\beta} = [Ц_{g,\beta}, C_{g,\beta}]$ – Марковская модель класса $\Phi_{g,\beta}$; $D_{g,\beta}$ – множество идентификаторов ФДП, составляющих класс $\Phi_{g,\beta}$; $Ц_{g,\beta}$ – матрица вероятностей переходов, соответствующая центру тяжести класса $\Phi_{g,\beta}$.

Различия в функциональных задачах пользователей и особенности процедуры формирования профилей приводят к тому, что профили пользователей имеют различное количество уровней. Это приводит к необходимости нормирования уровней информационных профилей различных пользователей с целью введения единой для ВИС многоуровневой системы контроля доступа. Для решения данной задачи вводится показатель степени безопасности действий пользователя. В связи с особенностями процедуры формирования профилей, наибольшей детализации (наибольший уровень информационного профиля) соответствует максимальный уровень контроля. Если максимальной степени безопасности действий пользователя поставить в соответствие единицу, то показатель степени безопасности действий пользователя, соответствующий уровню иерархии, определяется, как $C_\beta^u = \beta^u / Z^u$, где: β^u – уровень информационного профиля u-го пользователя, Z^u – наибольший номер уровня информационного профиля. В процессе контроля разграничения доступа в качестве эталонов действий пользователя выбираются элементы того уровня иерархического профиля, показатель степени безопасности которого наиболее близок (больше либо равен) заданному системой уровню контроля.

В целях своевременного выявления отклонения параметров наблюдаемой последовательности действий пользователя от полученных в результате формирования информационного профиля целесообразно ввести «контекст» контроля, представляющий собой последовательность событий доступа определенной длины, используемую для сравнения с эталоном. В целях соблюдения требований к достоверности контроля длина контекста контроля выбирается максимально возможной с учетом допустимых значений ошибок первого и второго рода.

Таким образом, применение информационных профилей пользователей позволяет реализовать в системе защиты информации ВИС механизм, обеспечивающий управление доступом к информационным ресурсам в контексте выполняемых пользователями задач, а также корректность их использования. Это позволяет существенно сократить возможности пользователей по нарушению безопасности информации.

Заключение

В целях контроля выполнения процедур безопасной обработки информации (сравнения текущего состояния процесса обработки информации с эталонными значениями профилей) могут быть применены

4-2017.indd 124 12.12.2017 11:25:51

методы последовательного анализа данных (обнаружения разладки), а также аппарат теории распознавания образов. Дальнейшие исследования предполагается проводить в следующих направлениях: разграничение доступа в облачных инфраструктурах [11]; применение механизма контроля доступа на основе профилей пользователей в целях проверки корректности настроек политики безопасности; выявление ранее неизвестных угроз безопасности в ВИС.

Литература

1. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президентом РФ от 05.12.2016 г. № 646.

2. Котенко, И. В. SIEM-системы для управления информацией и событиями безопасности / И.В. Котенко, И.Б. Саенко // Защита информации. Инсайд. – 2012. – № 5. – С. 54–65.

3. ГОСТ Р ИСО/МЭК ТО 13335-4-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер. –М.: Стандартинформ, 2007. – 64 с.

4. Авраменко, В. С. Адаптивный контроль защищенности информации от несанкционированного доступа на основе информационных образов / В.С. Авраменко // Проблемы информационной безопасности. Компьютерные системы. – 2010. – № 2. – С. 45–49.

5. Корт, С. С. Теоретические основы защиты информации: Учебное пособие / С.С. Корт. – М.: Гелиос АРВ, 2004. – 240 с.

6. Тихонов, В. И. Марковские процессы / В.И. Тихонов, М.А. Миронов. – М.: Советское радио, 1977. – 488 с.

7. Айвазян, С. А. Прикладная статистика и основы эконометрики / С.А. Айвазян, В.С. Мхитарян. – М.: ЮНИТИ, 1998. – 1006 с.

8. Мандель, И. Д. Кластерный анализ / И.Д. Мандель. – М.: Финансы и статистика, 1988. – 176 с.

9. Уиллиамс, У. Т. Методы иерархической классификации / У.Т. Уиллиамс, Д.Н. Ланс // Статистические методы для ЭВМ / Под ред. М. Б. Малютов. – М.: Наука, 1986. – С. 269–301.

10. Дуда, Р. О. Распознавание образов и анализ сцен / Р.О. Дуда, П.Е. Харт ; под ред. В. Л. Стефанюка. – М.: Мир, 1976. – 511 с.

11. Модель администрирования схем разграничения доступа в облачных инфраструктурах / И.Б. Саенко [и др.] // Информация и Космос. – 2017. – № 1. – С. 121–126.

4-2017.indd 125 12.12.2017 11:25:51