УДК 621.39

НЕКОТОРЫЕ ВОПРОСЫ РАЗРАБОТКИ МЕТОДОЛОГИИ ПОСТРОЕНИЯ СИСТЕМ КОНТРОЛЯ ДОСТУПА И ВЫБОРА ТЕХНОЛОГИИ ИДЕНТИФИКАЦИИ

В. В. Волхонский,
канд. техн. наук, доцент
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Рассмотрена модель системы контроля доступа с использованием теории множеств и понятия переходов. На ее основе сформулированы принципы построения таких систем как одного из основных элементов систем защиты объектов информатизации. Предложены критерии выбора технологии идентификации, позволяющие повысить надежность идентификации.

Ключевые слова *— контроль доступа, принципы построения, критерии выбора технологии идентификации.*

Введение

В настоящее время существует достаточно много работ по системам контроля и управления доступом (СКУД) [1–5], в которых рассматриваются различные аспекты функционирования таких систем. Однако это касается, главным образом, конкретных приложений и особенностей как самих систем контроля доступа, так и определенных видов идентификаторов. В то же время целесообразно сформулировать общие базовые принципы функционирования СКУД произвольной структуры, которые позволили бы использовать их при аппаратном и программном синтезе систем и оценке их параметров.

Разнообразие существующих, появление новых технологий идентификации и расширение спектра возможных задач идентификации практически на все стороны жизни общества (от антикражевых систем и систем идентификации товаров с групповыми идентификаторами до орнитологии, ихтиологии, задач пересылки почты и грузов, систем физической защиты объектов информатизации и хранения материальных ценностей и многих других) требуют обоснованного выбора той или иной технологии идентификации. Отсутствие объективных критериев выбора технологии идентификации для использования в конкретной задаче приводит к тому, что на практике такой выбор зачастую делается на основе эмпирических рассуждений, без учета объективных критериев. Такие критерии сформулированы лишь для частного случая биометрических идентификаторов [1]. Поэтому можно говорить о целесообразности формулировки критериев выбора технологии идентификации, которые, с одной стороны, являются общими, справедливыми для всех вариантов систем контроля доступа, а с другой стороны, учитывают особенности решаемых задач.

В целом решение перечисленных выше задач может послужить основой для разработки методологии построения СКУД.

Модель СКУД

Для описания СКУД можно использовать подход и модель [5], базирующиеся на представлении процесса функционирования СКУД в виде последовательности переходов, и математический аппарат теории множеств. При этом целесообразно модифицировать эту модель, используя подход, предложенный в работе [6] для системы охранной сигнализации как элемента системы физической защиты (СФЗ).

Использование единой модели для СКУД и СФЗ позволит, во-первых, в дальнейшем применять эту модель для интегрированных систем безопасности, включающих несколько подсистем, например контроля доступа и охранной сигнализации; во-вторых, полнее учесть особенности СКУД, в частности, реализовать привязку модели к вре-

менным параметрам для контроля нахождения субъекта доступа в зонах контролируемого доступа. А это необходимо для учета уровня доступа $\mathbf{У}_k$ для k-го субъекта доступа, определяемого как совокупность $\mathbf{У}_k = \{\mathbf{D}_k, \Delta\mathbf{t}_k, \Delta\mathbf{T}_k, \mathbf{R}\}$ разрешенных точек доступа $\mathbf{D}_k$ и соответствующих им разрешенных временных $\Delta\mathbf{t}_k$ и календарных $\Delta\mathbf{T}_k$ интервалов, а также уровня $\mathbf{R}$ угрозы.

Совокупность точек доступа d_i всей СКУД может быть определена множеством $\mathbf{D}^{\text{СКУД}}$, которому принадлежат эти точки доступа: $d_i \in \mathbf{D}^{\text{СКУД}}$, $i = 1, ..., I$. Обычно специфика реальных объектов такова, что имеется несколько структурных подразделений (цехов, зданий, отделов, ...) с разными режимами функционирования и уровнями доступа в каждое из них. Кроме того, аппаратные средства СКУД, как правило, используют несколько контроллеров, которые могут иметь определенные функциональные ограничения на работу групп точек доступа, которые они обеспечивают. Следовательно, в общем случае, с учетом таких возможных функциональных особенностей объекта и оборудования, в СКУД могут иметь место несколько разделов, отличающихся уровнями доступа пользователей. Поэтому множество $\mathbf{D}^{\text{СКУД}}$, в свою очередь, разделяется на $M_{\text{р}}^{\text{СКУД}}$ подмножеств точек доступа разделов $\mathbf{D}_m^{\text{СКУД}}$, где $m = 1, ..., M_{\text{р}}^{\text{СКУД}}$. Подмножества точек доступа $\mathbf{D}_m^{\text{СКУД}}$ могут быть как пересекающимися, так и непересекающимися. Это зависит от структуры СКУД, в частности, от структуры зон доступа [5] (последовательные, параллельные, вложенные, пересекающиеся) и от того, имеют ли упомянутые структурные подразделения общие зоны доступа и, соответственно, общие точки доступа. Поэтому можно записать выражение $\mathbf{D}_1^{\text{СКУД}} \cup \mathbf{D}_2^{\text{СКУД}} ... \cup \cup \mathbf{D}_M^{\text{СКУД}} = \mathbf{D}^{\text{СКУД}}$, определяющее соотношение между подмножествами $\mathbf{D}_m^{\text{СКУД}}$ и $\mathbf{D}^{\text{СКУД}}$.

Аналогично совокупность зон z_j доступа, контролируемых СКУД, может быть определена множеством $\mathbf{Z}^{\text{СКУД}}$, которому принадлежат точки доступа $z_j \in \mathbf{Z}^{\text{СКУД}}$. Учитывая упомянутую выше специфику объектов (возможное наличие разделов), множество $\mathbf{Z}$ будет состоять из $L_{\text{р}}^{\text{СКУД}}$ подмножеств $\mathbf{Z}_l^{\text{СКУД}}$, $l = 1, ..., L_{\text{р}}^{\text{СКУД}}$, с элементами z_j.

Для возможности использовать модель работы [6] учтем следующее. В СФЗ основными элементами, позволяющими регулировать продолжительность проникновения, являются препятствия, определяемые множеством $\mathbf{D}^{\text{СФЗ}}$. Основными элементами СКУД, определяющими режим ее функционирования, являются точки доступа. Для применимости используемой модели [6] к системе контроля доступа необходимо учесть взаимосвязь между $\mathbf{D}^{\text{СФЗ}}$ и $\mathbf{D}^{\text{СКУД}}$. Препятствия СФЗ в СКУД можно рассматривать не только как элементы точек доступа (например, двери, оснащенные считывателями и элементами управления доступом), но и как зоны доступа (двери, не оборудованные средствами СКУД). То есть такие элементы, как препятствия, могут быть отнесены в СКУД либо к зонам, либо к точкам доступа. При этом все точки доступа (элементы множества $\mathbf{D}^{\text{СКУД}}$) применительно к СКУД являются препятствиями, но не все препятствия (элементы множества $\mathbf{D}^{\text{СФЗ}}$) являются точками доступа, т. е. $\mathbf{D}^{\text{СФЗ}} \in \mathbf{D}^{\text{СКУД}}$. Таким образом, характерными точками СКУД являются зоны контролируемого доступа (как аналог охраняемых зон в СФЗ) и точки доступа (как аналог препятствий СФЗ).

Переходы субъекта доступа

Субъект доступа может перемещаться по объекту из одной зоны в другую и преодолевать точки доступа по определенному пути или маршруту. Такое перемещение может быть представлено с помощью последовательности переходов между характерными точками объекта, аналогичной используемой в работах [5, 6]. В качестве характерных точек маршрута могут быть выбраны начало и конец зоны доступа или точки доступа. Перемещения субъекта доступа между такими точками можно трактовать как переходы. В этом случае будут иметь место два основных типа переходов — по контролируемой зоне до точки доступа и через точку доступа с переходом в контролируемую зону.

Введем обозначение перехода c_{ij}, которое может соответствовать следующим вариантам: переходу от начала i-й зоны до начала j-й точки доступа или преодолению i-й точки доступа с переходом в j-ю зону доступа.

Нулевой индекс будет обозначать зону свободного доступа. Таким образом, в общем случае переход c_{ij} означает следующее. При $i \neq 0$, $j = 0$ — перемещение субъекта доступа из i-й зоны контролируемого доступа в j-ю зону свободного доступа. При $i = 0$, $j \neq 0$ — перемещение субъекта доступа из зоны свободного доступа в j-ю зону контролируемого доступа. При $i = j$ — возврат в ту же самую зону доступа (контролируемого или свободного) с идентификацией в точке доступа, но без перемещения через эту точку доступа. Переходы c_{ij} и c_{ji} с разным порядком следования индексов отличаются порядком (направлением) прохождения точек доступа.

В зависимости от решаемой задачи возможны различные варианты сочетания количества зон и точек доступа, от которых будут зависеть представления маршрута субъекта доступа:

1) произвольные совокупности точек и зон доступа (несовпадающее их количество);

2) связанные пары точка/зона доступа (совпадающее количество);

3) совокупность только точек доступа.

Первый вариант представления является наиболее общим, и использовать его имеет смысл, когда зону между двумя точками доступа по какой-либо причине удобнее разбить на несколько отдельных зон. Например, если возможны разветвления маршрута на участках между точками доступа. В частности, когда есть несколько точек доступа между одними и теми же зонами. Во втором варианте количество точек и зон доступа между ними совпадает. Третий является частным случаем первых двух, когда время прохождения зон пренебрежимо мало по сравнению со временем прохождения точек доступа, либо для СКУД без контроля нахождения субъекта доступа в зоне контролируемого доступа.

Если необходимо, к примеру, моделировать СКУД с учетом времени нахождения в зоне контролируемого доступа, то нужен учет зон доступа $\mathbf{Z}^{\text{СКУД}}$; если без учета — то множество $\mathbf{Z}^{\text{СКУД}}$ можно считать пустым: $\mathbf{Z}^{\text{СКУД}} = \varnothing$.

Рассмотрим описание переходов для различных вариантов сочетаний точек и зон доступа.

Произвольные совокупности точек и зон доступа.

Совокупность всех возможных переходов c_{ij}, $i, j = 0, ..., I, I + 1, ..., I + J$, составляет множество $\mathbf{C}$ переходов. Значение индекса «0» соответствует зоне свободного доступа или нахождению вне контролируемого объекта. Эта совокупность может быть представлена квадратной матрицей $\mathbf{C}_{IJ}$ с количеством строк и столбцов, определяемым суммой количества точек I и зон J доступа:

$$\mathbf{C}_{IJ} = \begin{bmatrix} c_{00} & c_{10} & \cdots & c_{I-1,0} & c_{I,0} & c_{I+1,0} & \cdots & c_{I+J,0} \\ c_{01} & \cdots & & & & & \cdots & c_{I+J,1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ c_{0,I} & c_{1,I} & \cdots & & c_{I,I} & c_{I+1,I} & \cdots & c_{I+J,I} \\ c_{0,I+1} & c_{1,I+1} & \cdots & & c_{I,I+1} & c_{I+1,I+1} & \cdots & c_{I+J,I+1} \\ c_{0,I+2} & & \cdots & & & & \cdots & c_{I+J,I+2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ c_{0,I+J} & c_{1,I+J} & \cdots & & c_{I,I+J} & c_{I+1,I+J} & \cdots & c_{I+J,I+J} \end{bmatrix}. \quad (1)$$

Элементы этой матрицы в простейшем случае определяют возможность выполнения перехода. Они равны единице при наличии такой возможности: $c_{ij} = \begin{cases} \mathbf{0}, c_{ij} \notin \mathbf{C} \\ \mathbf{1}, c_{ij} \in \mathbf{C} \end{cases}$, и равны нулю при ее отсутствии.

Связанные пары точка/зона доступа.

Для случая связанных пар точка/зона, т. е. при совпадающем количестве точек и зон доступа, матрица $\mathbf{C}_{IJ}$ возможных переходов упрощается и принимает вид $\mathbf{C}_{II}$, аналогичный (1) с учетом равных значений $I = J$.

Совокупность только точек доступа.

Для третьего случая учета только точек доступа матрица $\mathbf{C}_{IJ}$ будет иметь меньшее количество элементов, определяемое только количеством I точек доступа:

$$\mathbf{C}_I = \begin{bmatrix} c_{00} & c_{10} & \cdots & c_{I,0} \\ c_{01} & \cdots & & c_{I,1} \\ \cdots & \cdots & \cdots & \cdots \\ c_{0,I} & c_{1,I} & \cdots & c_{I,I} \end{bmatrix}. \quad (2)$$

Во всех упомянутых выше ситуациях могут быть частные случаи.

1. Когда не контролируется направление перехода через точку доступа, т. е. не различаются переходы в прямом c_{ij} и обратном c_{ji} направлениях. Тогда в матрице

$$\mathbf{C}_I = \begin{bmatrix} c_{00} & c_{01} & \cdots & c_{0,I} \\ c_{01} & \cdots & & c_{1,I} \\ \cdots & \cdots & \cdots & \cdots \\ c_{0,I} & c_{1,I} & \cdots & c_{I,I} \end{bmatrix}$$

элементы над и под диагональю попарно равны.

2. При одностороннем контроле доступа учитываются только переходы c_{ij} и не учитываются c_{ji}. Тогда часть элементов матрицы $\mathbf{C}_I$ становятся равными нулю и будут выглядеть, к примеру, следующим образом:

$$\mathbf{C}_I = \begin{bmatrix} c_{00} & 0 & \dots & c_{I,0} \\ c_{01} & \dots & & c_{I,1} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & c_{I,I} \end{bmatrix}.$$

Либо, в случае последовательного выбора порядка точек и зон доступа, матрица $\mathbf{C}_I$ будет иметь нулевые элементы выше или ниже диагонали:

$$\mathbf{C}_I = \begin{bmatrix} c_{00} & 0 & \dots & 0 \\ c_{01} & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots \\ c_{0,I} & c_{1,I} & \dots & c_{I,I} \end{bmatrix}.$$

Маршруты субъекта доступа

С точки зрения введенного понятия переходов, маршрут R_n субъекта доступа представляет собой определенную конечную чередующуюся последовательность переходов. Таким образом, n-й маршрут R_n включает в себя подмножество $\mathbf{C}_n$ множества $\mathbf{C}$ возможных переходов. Сформулируем понятие маршрута субъекта доступа на основе определений, касающихся маршрутов [5].

Маршрут субъекта доступа — это конечная последовательность переходов, выполненных им. С учетом используемых обозначений маршрут может быть записан как $R_n = \{c_{ij}, ..., c_{km}, c_{ml}\}$.

Непрерывный маршрут включает все последовательно выполняемые переходы на маршруте движения субъекта доступа без пропуска: $R_n = \{c_{ij}, c_{jk}, ..., c_{km}, c_{ml}\}$.

Замкнутый маршрут начинается и заканчивается в одной и той же зоне доступа: $R_n = \{c_{ij}, c_{jk}, ..., c_{km}, c_{mi}\}$. Маршрут может быть *квазизамкнутым*: $R_n = \{c_{0j}, c_{jk}, ..., c_{km}, c_{i0}\}$, когда субъект доступа перемещается в зону контролируемого доступа из зоны свободного доступа через одну внешнюю точку доступа, а выходит также в зоне свободного доступа, но через другую внешнюю точку доступа. В противном случае маршрут считается *открытым*.

Полный маршрут начинается и оканчивается на внешних концевых зонах свободного доступа и включает в себя все переходы, выполненные на объекте в зонах контролируемого доступа: $R_n = \{c_{0j}, c_{jk}, ..., c_{km}, c_{m0}\}$.

Полный замкнутый маршрут начинается и заканчивается в одной и той же внешней концевой зоне свободного доступа: $R_n = \{c_{0j}, c_{jk}, ..., c_{kj}, c_{j0}\}$. То есть в частном случае полного маршрута концевые зоны доступа являются внешними зонами свободного доступа.

Очевидно, что, с общей точки зрения построения СКУД, корректный маршрут субъекта доступа должен быть полным, непрерывным и замкнутым (квазизамкнутым), т. е. субъект должен пройти все последовательно связанные зоны и соответствующие им точки доступа на данном маршруте.

Основные принципы функционирования СКУД

На основе анализа рассмотренной выше модели СКУД можно сформулировать принципы функционирования СКУД, которые надо соблюдать при разработке таких систем.

1. *Санкционированность* — любые действия в СКУД должны подтверждаться соответствующим уровнем доступа. Принцип выглядит, возможно, тривиальным и «де-факто» используется в профессиональных СКУД, например, для выявления попыток несанкционированного доступа подбором идентификаторов, но не всегда реализуется в реальных системах.

2. *Неповторяемость* — прохождение одной и той же точки доступа не может быть выполнено дважды подряд в одном и том же направлении без прохождения других точек доступа или этой же точки доступа в противоположном направлении. Это так называемый контроль повторного прохода [3, 4]. Однако на практике он не всегда используется или имеет ограниченный функционал — позволяет выявлять попытки повторного прохода только в пределах ограниченной группы точек доступа раздела, а не во всей системе. Эта группа обычно определяется параметрами одного контроллера СКУД. Выполнение этого принципа иногда не контролируется в упрощенных системах, что приводит к снижению надежности СКУД.

3. *Непрерывность* — санкционированное перемещение через точки доступа должно осуществляться только с последовательным прохождением подряд всех связанных зон и соответствующих принадлежащих этим зонам точек доступа без пропуска на данном маршруте. Выполнение этого принципа соответствует непрерывному маршруту субъекта доступа.

4. *Замкнутость* — любой корректный маршрут должен быть замкнутым (квазизамкнутым) в пределах временных Δt_k и календарных ΔT_k интервалов, определяемых уровнем доступа $У_k$. Это соответствует полному замкнутому или квазизамкнутому маршрутам, рассмотренным выше.

5. *Осуществимость* — корректное перемещение объекта должно осуществляться только по конструктивно и (или) организационно предназначенным для этого маршрутам. Например, при проникновении на территорию предприятия через ограждение периметра (т. е. при нарушении режима функционирования СКУД) и выходе таким же образом маршрут субъекта доступа может быть замкнутым и непрерывным, т. е. удовлетворяющим п. 4 и 5, но не являться полным. Таким образом, условия 4 и 5 являются необходимыми, но не достаточными.

6. *Монотонность*:

• уровень доступа в каждую из последующих последовательно связанных зон должен быть выше предыдущей. Иначе, возможно, уровень доступа занижен или нет необходимости в точке доступа, и зоны могут быть объединены;

• для последовательно связанных зон субъект доступа, имеющий i-й уровень доступа (позволяющий перемещение через i-ю точку доступа), должен иметь и $(i - 1)$-й уровень доступа (для $i > 1$).

Последнее правило справедливо и может использоваться только для сравнимых уровней доступа [5].

Критерии выбора технологии идентификации

Сформулируем общие критерии выбора технологии идентификации. В работе [1] приводятся критерии выбора биометрических идентификационных признаков, т. е. для частного случая определенной технологии идентификации. Отметим, что эти критерии справедливы не только для биометрических идентификаторов и их можно рассматривать как часть общего списка критериев выбора для произвольной СКУД. Аналогичные русскоязычные термины могут быть записаны следующим образом.

Неповторяемость — идентификационные признаки не должны полностью повторяться у любых субъектов или объектов доступа. Исключением служат СКУД с групповыми идентификаторами.

Стабильность — идентификационные признаки должны оставаться неизменными во времени. Или, точнее, изменения не должны выходить за допустимые пределы, приводящие к нарушению любого из рассматриваемых критериев.

Считываемость — должна обеспечиваться возможность беспрепятственного считывания этих признаков современными техническими средствами. Например, размещение идентификатора со штрих-кодом в пластиковый держатель может приводить к сбоям в работе оптического считывателя за счет дополнительного рассеивания светового потока.

Доступность — возможность получения этих признаков без каких-либо юридических, этических, моральных и других норм и правил.

Наличие — признаки должны присутствовать у всех СОД.

Однако задачи синтеза и анализа СКУД требуют формулировки критериев выбора технологии (метода и способа) идентификации для произвольного субъекта или объекта доступа и произвольных идентификаторов (различных по физическому принципу действия и набору технических параметров). Эти критерии могут быть сформулированы следующим образом.

Присваиваемость — возможность присвоения идентификатора определенному субъекту. Так, могут потребоваться дополнительные технические средства для присвоения идентификатора, например держатель карты доступа.

Приемлемость — согласие субъекта или объекта доступа на присвоение определенного идентификационного признака. Термин «согласие» надо понимать в обобщенном виде. Это может быть согласие субъекта доступа в полном смысле этого слова, или отсутствие того или иного вида отторжения идентификатора объектом доступа (например, в орнитологии или ихтиологии), либо приемлемость для владельца или пользователя этого объекта.

Законность — соответствие законам страны и правилам административной территории или ведомственным требованиям организации, эксплуатирующей СКУД.

Защищенность — обеспечение защищенности идентификатора и (или) идентификационных признаков от различных факторов, к которым можно отнести перечисленные в ГОСТ [7] манипулирование, копирование, наблюдение. Должна обеспечиваться защищенность также от угроз идентификаторам, не упомянутых в стандарте, таких как съем информации о них, воздействие естественных и искусственных факторов (электромагнитных излучений, магнитных полей и т. п.), приводящих к нарушению целостности идентифи-

фикаторов, идентификационных характеристик и признаков, к их частичной или полной потере. Кроме того, в упомянутом стандарте не указана и такая угроза, как кража идентификатора.

Принадлежность — обеспечение однозначной принадлежности идентификатора или идентификационных признаков субъекту или объекту доступа, не допускающей использования этого идентификатора или идентификационных признаков другим субъектом или объектом доступа. Например, переклеивания идентификатора товара или идентификатора проведения досмотра багажа в аэропорту.

Достаточность — возможность принятия однозначного решения или решения с заданными вероятностями об идентификации данного объекта или субъекта доступа и предоставления ему доступа или отказа в нем. К примеру, при идентификации по отпечатку пальца реально используется информация лишь о части характерных точек папиллярных узоров.

Реализация приведенных выше критериев при синтезе СКУД позволит повысить эффективность системы.

Заключение

На основе представления СКУД в терминах теории множеств, позволяющего формализовать маршрут перемещения субъекта доступа как конечную чередующуюся последовательность зон и точек доступа и переходов между ними и через них, сформулированы принципы функционирования СКУД: санкционированность, неповторяемость, непрерывность, замкнутость, осуществимость и монотонность.

Предложен подход, позволяющий использовать один и тот же математический аппарат и единую модель для различных подсистем безопасности, в частности, подсистем охранной сигнализации и контроля доступа. Этот подход может быть распространен и на другие типы подсистем.

В дополнение к известным критериям, которым должны соответствовать биометрические идентификационные признаки, сформулированы критерии выбора технологии идентификации для произвольного субъекта или объекта доступа: достаточность, защищенность, принадлежность, присваиваемость, приемлемость и законность.

Литература

1. **Wayman J., Jain A., Malton D., Maio D.** Biometric Systems. Technology, Design and Performance Evaluation. London: Springer. — 2005. — 374 p.
2. **Finkenzeller K.** RFID Handbook. Fundamentals and Applications in Contactless Smart Cards and Identification. Sec. ed. — Munich: Giesecke & Devrient GmbH, 2003. — 427 p.
3. **Оленин Ю. А., Шестаков К. И.** Метод принятия решения в системах контроля и управления доступом при реализации функции antipassback. Ч. 2 // Системы безопасности. 2001. Октябрь—ноябрь. С. 32–33.
4. **Оленин Ю. А., Шестаков К. И.** Метод принятия решения в системах контроля и управления доступом при реализации функции antipassback. Ч. 1 // Системы безопасности. 2001. Август—сентябрь. С. 36–37.
5. **Волковицкий В. Д., Волхонский В. В.** Системы контроля и управления доступом. — СПб.: Экополис и культура. — 2003. — 165 с.
6. **Волхонский В. В., Гатчин Ю. А.** Подход к задаче анализа эффективности системы безопасности на основе вероятностных оценок временных параметров процесса проникновения на защищаемый объект // Вестник компьютерных и информационных технологий. 2012. № 2. С. 35–39.
7. **ГОСТ Р 51241–2008.** Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. — М.: Госстандарт России, 2008. — 32 с.