4. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».
5. Указ Президента Российской Федерации от 23.09.2005 г. №1111 «Перечень сведений конфиденциального характера».
6. *Миронова В.Г., Шелупанов А.А.* Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности // Докл. Том. гос. ун-та систем управления и радиоэлектроники. – 2010. – № 2 (22). – Ч. 1. – С. 257-259.

Статью рекомендовал к опубликованию к.ф.-м.н. Г.А. Афонин.

Миронова Валентина Григорьевна
Томский государственный университет систем управления и радиоэлектроники.
E-mail: mvg@security.tomsk.ru.
634050, г. Томск, пр. Ленина, 40.
Тел.: 89234151608.
Кафедра комплексного обеспечения информационной безопасности электронно-вычислительных систем; аспирант.

Шелупанов Александр Александрович
E-mail: saa@udcs.ru.
Проректор по научной работе; д.т.н.; профессор.

Mironova Valentina Grigor'evna
Tomsk State University of Control Systems and Radioelectronics.
E-mail: mvg@security.tomsk.ru.
40, Lenin Pr., Tomsk, 634050, Russia.
Phone: +79234151608.
The Departmant of Integrated Information Security Computer Systems; Postgraduate Student.

Shelupanov Alexander Alexandrovich
E-mail: saa@udcs.ru.
Vice Rector for Research; Dr. of Eng. Sc.; Professor.

УДК 004.05

О.М. Лепешкин, Р.С. Гаппоев

МАНДАТНАЯ МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА НА ОСНОВЕ СРЕДЫ РАДИКАЛОВ

Исследование в области защиты информации и вычислительной техники показывает, что в развитых странах мира уже давно сложилась инфраструктура безопасности информации в системах обработки данных, которая нуждается в рассмотрении для систем реального времени. Внедрение системных требований международных стандартов и принципов процессного подхода в системы управления, приводит к изменению принципов контроля безопасности и требует пересмотра основных подходов по построению систем безопасности в динамике.

Вследствие этого, в данной статье проведен анализ основных моделей разграничения доступа на основе мандатной политики безопасности: «Белла – Лападула» и «Китайской стены», для систем реального времени. Выявлены основные недостатки и противоречия (деклассификация объектов) этих моделей, которые потенциально могут нарушать безопасность системы. Для устранения этих проблем предлагается рассмотреть модель предоставления прав доступа на основе «полномочий субъекта» и «допуска полномочий у объекта». Для реализации данного метода было решено использовать среду радикалов, основой которых являются предикаты.

Политика безопасности; мандатные модели; мандатный доступ; контроль целостности; схемы радикалов.

O.M. Lepeshkin, R.S. Gappoev

MANDATORY ACCESS CONTROL THROUGH DIAGRAMS OF RADICALS

Research in the field of information and computer technology shows that in the developed world have long formed the infrastructure of information security in data processing systems, which need to be considered for real-time systems. The introduction of the system requirements of international standards and principles of the process approach to management leads to a change in the principles of security controls and requires a review of the main approaches to the construction of security systems in the dynamics.

Consequently, this paper analyzes the basic models of access control based on the mandatory security policy, "Bell - LaPadula," and "Chinese walls" for real-time systems. The basic flaws and contradictions (unclassification objects) of these models that could potentially violate the security of the system. To address these issues is invited to consider the model of providing access to truths based on the "authority of the subject" and "admission authority for the object." To implement this method, it was decided to use the medium of radicals, which are based predicates.

Security policy; the mandatory models; the mandatory access; control of integrity; diagrams of radicals.

Исследование в области защиты информации и вычислительной техники показывает, что в развитых странах мира уже давно сложилась инфраструктура безопасности информации в системах обработки данных, которая нуждается в рассмотрении для систем реального времени. Внедрение системных требований международных стандартов и принципов процессного подхода в системы управления, приводит к изменению принципов контроля безопасности и требует пересмотра основных подходов по построению систем безопасности в динамике. Существующие подходы ориентированы в основном на этап проектирования и не в полной мере учитывают динамику процесса. В большинстве случаев необходимый уровень защищенности достигался за счет делегирования прав доступа, основанных на статической политике безопасности, что нередко приводило к снижению целостности информации, из-за отсутствия контроля в реальном масштабе времени. Вследствие этого, в данной статье предлагается провести анализ моделей мандатной политики, которая состоит из мандатных моделей и моделей контроля целостности, выявление основных противоречий в этих моделях, а также определение основных направлений, которые позволят устранить данные недостатки.

Мандатные модели безопасности – это модели безопасности, в которых управление доступом основано на уровнях и категориях целостности и разграничении доступа субъектов к объектам, основываемое на характеризуемой метке конфиденциальности информации, содержащейся в объектах и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Классическими мандатными моделями безопасности являются модель «Белла – Лападула» и «Китайская стена». Алгоритмы этих моделей просты и эффективны, что является основными их достоинства. К примеру, простое правило NWD(No Write Down) разрешает проблему троянских коней, так как запись информации на более низкий уровень секретности, типичная для троянских коней операция, запрещена.

Несмотря на все достоинства, при использовании модели «Белла – Лападула» в контексте практического проектирования и разработки реальных компьютерных систем возникает техническая проблема, так называемая деклассификация объекта. Допустим, субъект с уровнем секретности «совершенно секретно» получил доступ к файлу с грифом также «совершенно секретно», после чего он понизил свой уровень секретности до «секретно» или даже «для служебного пользования» – формально он имеет на это право и мандатную модель это не нарушает. После

этого субъект записывает информацию в файл с грифом «секретно» или «для служебного пользования» (он ведь находится на одном с ними уровне) – безопасность системы нарушена, но требования и условия модели «Белла – Лападулы» формально соблюдены [1].

Однако реализация системного и процессного подходов требуют учета безопасности доступа субъектов и объектов на основе выполняемых функций и задач системой в реальном масштабе времени. Следовательно, при организации доступа должны учитываться процессные состояния системы и взаимосвязь объектов и субъектов доступа по функциям и задачам, чтобы исключить самопроизвольное изменение уровня секретности и тем самым провести деклассификацию объекта.

Модель не учитывает разграничения доступа в условиях выполнения коллективных задач, когда в реальном масштабе времени имеют доступ субъекты с различными уровнями секретности к одним и тем же функциям и задачам системы. Субъекты заданного уровня секретности одновременно как по времени, так и по задачам и функциям, выполняющимся в реальном масштабе времени имеет доступ к системе без ограничения. Это снова противоречит принципам безопасности и требует пересмотра основных подходов построения мандатных моделей для процессного подхода.

Современный математический аппарат, реализующий систему описания мандатного доступа, не позволяет реализовать данные требования, т.е. рассмотрение моделей в динамике, а не в статике, что требует разработки новых математических подходов по устранению данных недостатков.

В заключение общей характеристики мандатных моделей отметим, что анализ самих моделей не может оцениваться количественными показателями, так как их построение основывается на теории множеств, что делает невозможным данные оценки. В мандатных моделях разграничение доступа осуществляется до уровня классов безопасности сущностей системы: любой объект определенного уровня безопасности доступен любому субъекту соответствующего уровня безопасности (с учетом правил NRU и NWD). Следовательно, мандатный подход к разграничению доступа, основываясь только лишь на идеологии градуированного доверия, без учета специфики характеристик субъектов и объектов в процессе их функционирования, что приводит в большинстве случаев к избыточности прав доступа для конкретных субъектов в пределах соответствующих классов безопасности, противоречит самому понятию разграничения доступа.

Для устранения данного недостатка мандатный принцип доступа дополняется дискреционным внутри. В теоретических моделях для этого вводят матрицу доступа, разграничивающую разрешенный по мандатному принципу доступ к объектам одного уровня безопасности, но при этом ситуация только усложняется, так как в дискреционном подходе есть свои существенные недостатки [2].

Как показано на рис. 1, каждый субъект имеет набор полномочий. Состав этого набора позволяет ему исполнять определенные функции относительно объекта. В то же время и объект обладает определенным составом допуска полномочий, которые также впоследствии позволяют субъекту производить действия над объектом. Этот набор полномочий фактически представляет собой совокупность ролей относительно каждого объекта («объект 1 – чтение», «объект 2 – запись» и.т.п.), которые в последствии сопоставляются с допуском полномочий объекта. Так в данной модели будет реализоваться основная политика безопасности мандатная, внутри которой будет дискреционная (разделение субъектов по полномочиям к каждому объекту).

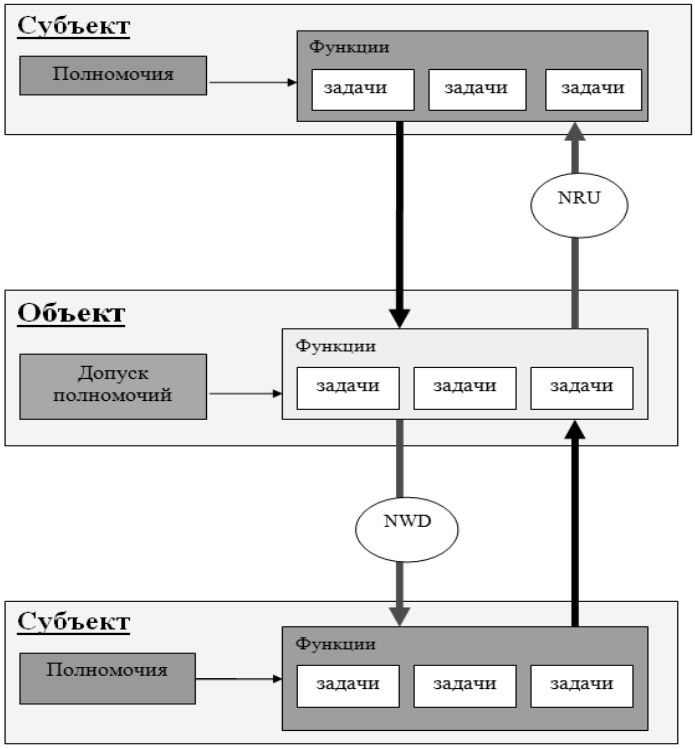

Рис. 1. Схема организации мандатного доступа

Этот описательный подход помогает решать проблему деклассификации объектов, так как теперь доступ не зависит от уровня доступа субъекта, а зависит от набора полномочий относительно функций субъекта. Важно теперь продумать математический аппарат, который позволит внедрить и использовать данный метод. Поэтому предлагается использовать один из основных подходов к обеспечению информационно-системной безопасности (ИСБ) сложных систем – интеллектуализацию таких систем. Интеллектуализация любой системы подразумевает оснащение системы элементами интеллекта, создание у нее специального информационно-программного окружения с целью обеспечения ИСБ поведения этой системы в рамках ее метасистемы. Такое оснащение должно обеспечивать постоянную адаптацию сложной системы к изменяющимся внутренним и внешним условиям, проводить диагностику, контроль, анализ и синтез отдельных составляющих системы и функционирования системы в целом с учетом последствий этого функционирования с целью обеспечения ИСБ поведения системы на протяжении всего ее жизненного цикла.

Для реализации этого подхода (интеллектуализации) предлагается использовать среду радикалов, основой которых являются предикаты. Рассмотрим метод ухода от конфликтов доступа ИУС на основе среды радикалов [3].

Радикал – это функциональная система, имеющая два типа состояний – пассивное и активное. Активный радикал – это система, выполняющая свою функцию. Пассивный радикал – это та же система, но не выполняющая своей функции, как бы отключенная. Радикалы организованы в среду радикалов и требуют своего естественного дополнения в форме активаторов. Среда радикалов реализуется средствами специализированной системы (стенда) обеспечения комплексных раз-

работок (СОКР) сложной системы и образует основу рабочей подсистемы СОКР. В состав СОКР входит также активирующая подсистема, которая осуществляет выбор и последующую активацию тех или иных радикалов. Благодаря согласованному функционированию активирующей и рабочей подсистем СОКР, реализуется процесс решения задач жизненного цикла сложной системы.

ИСБ сложной системы обеспечивается с помощью математического моделирования в форме нормализации среды радикалов проблемной области. Нормализация – это МС, которое проводится в три этапа. Так на начальном этапе(первый этап нормализации) происходит разделение радикалов на два вида: уникумы и контейнеры. Уникум – это объект проблемной области, например, составляющая сложной системы. Контейнер – способ задания связи определенного типа между радикалами, например, свойство уникума.

На основе этого разделения, метод ухода конфликтов доступа ИУС позволяет решать задачу реализации доступа уникума, характерную для всех этапов жизненного цикла сложной системы и называется **двунаправленным методом синтеза доступа уникума**. Пусть требуется построить уникум uGoal (рис. 2). Это может быть сложная система, ее составляющая, некоторое управляющее воздействие, уводящее систему от конфликта. Требования к уникуму uGoal определяются целевыми контейнерами. Построение осуществляется с помощью библиотеки стандартных радикалов (третий этап нормализации).

Если существует уже реализованный библиотечный уникум доступа, удовлетворяющий целевым контейнерам, то задача решена.

Однако, если такого уникума не существует, тогда из библиотеки, с помощью ультра контейнеров, выбираются уникумы (со своими контейнерами), про которые можно предположить, что, будучи связаны друг с другом (при помощи контейнеров) определенным допустимым образом, они реализуют целевой уникум (осуществляется "проход вниз".)

Эти уникумы обычно являются "обобщенными составляющими", т.е. представляют классы составляющих системы. Обозначим эти уникумы ui_1, …, ui_n. (uVi – один из вариантов реализации целевого уникума на первом уровне). Уникумы ui_1, …, ui_n находятся в библиотеке вместе с контейнерами, характеризующими их, образно говоря, как "по горизонтали", так и "по вертикали", т.е. в библиотеке должны быть описаны как все допустимые "среды доступа и структура" для этих уникумов, так и требования к их реализации. Пусть также в библиотеке имеются ультра-контейнеры, с помощью которых по уникумам ui_1, …,ui_n можно определить контейнеры, характеризующие вариант uVi для целевого уникума uGoal.

Теперь надо реализовать каждый из этих n уникумов доступа. Пусть имеются ультра-контейнеры, позволяющие определить целевые контейнеры для каждого из этих уникумов, в том числе и для уникума ui_1. Таким образом, теперь задача построения уникума решается для этого уникума ui_1 и для всех остальных уникумов ui_2, …, ui_n. Причем каждый раз контейнеры верхних уровней, в общем случае, корректируются (т.е. осуществляются "проходы вверх").

Так можно дойти до использования в иерархии уже реализованных библиотечных уникумов uBuilt* (с соответствующими контейнерами). Пусть в нашем случае это произойдет для уникума ui_1. Теперь будем двигаться вверх. Сначала получим контейнеры, реализованные для этого уникума ui_1 (с помощью уникумов uBuilt*).

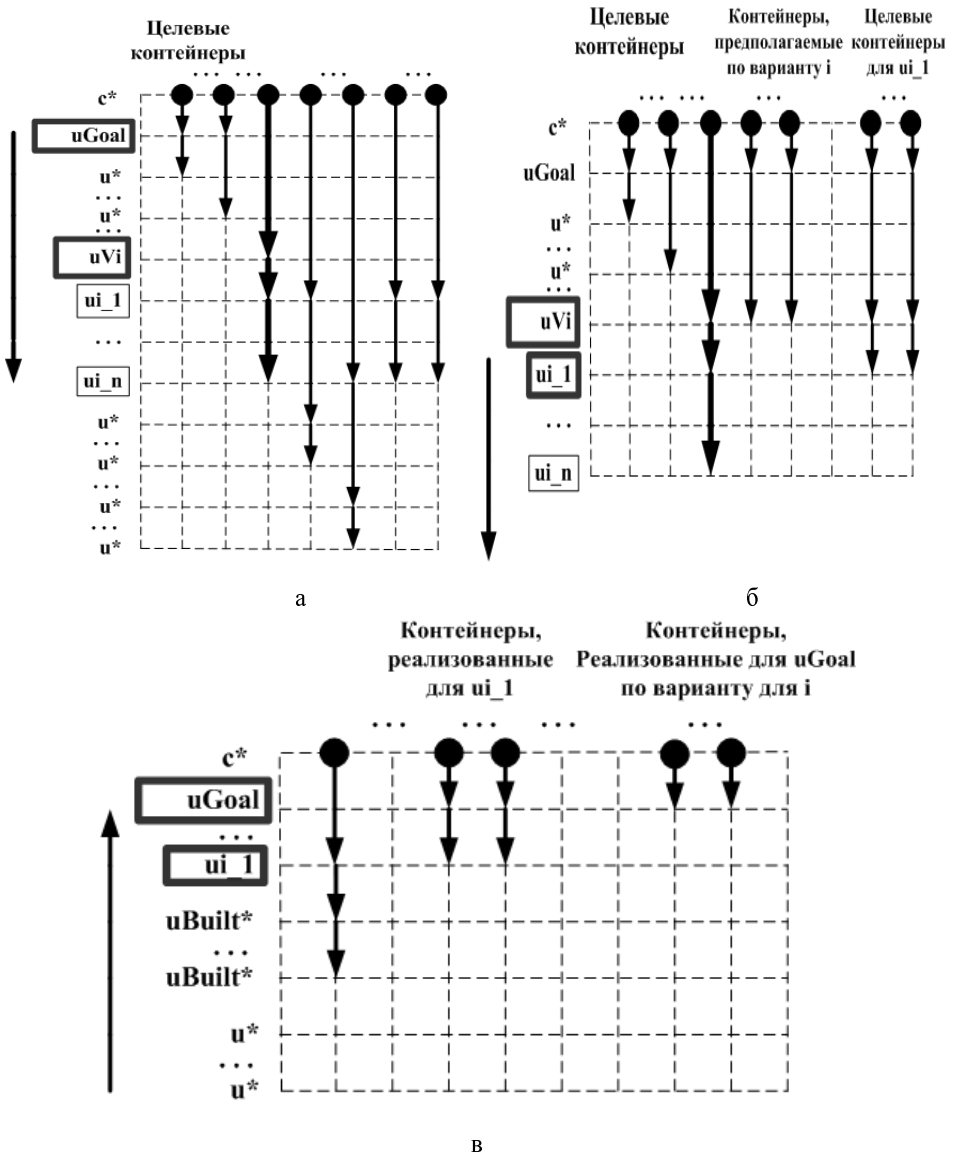

Рис. 2. Схемы построения уникума uGoal

Будем продолжать доступ вверх, корректируя полученные ранее контейнеры. Действуя таким образом, для всех уникумом ui_*, получим контейнеры, реализованные для исходного целевого уникума uGoal по i-му варианту с помощью реализованных ранее уникумов uBuilt*.

Для любого целевого уникума доступа и характеризующей его схемы, и любой библиотеки стандартных радикалов, представленных нормализованными системами векторов, существует конечная последовательность шагов применения двунаправленного метода построения уникума, с помощью которой: либо осуществимо построение конечного числа доступов, реализующих целевой уникум; либо делается вывод о том, что при данной библиотеке стандартных радикалов целевой уникум доступа нереализуем.

Качество предлагаемого формально-методического аппарата и его эффективность удобно продемонстрировать на характерном примере его применения. Рассмотрим сложную систему, на некотором этапе ее жизненного цикла. Система реализована с помощью иерархии, состоящей из многих составляющих. Пусть каждая составляющая характеризуется множеством контейнеров (ультраконтейнеров), согласно чему фиксируется принадлежность этой составляющей множеству классов доступа. Для фиксации классов доступа, которым принадлежит составляющая, используются контейнеры вида cClassOfScheme. Для классификации составляющих по множествам классов, которым каждая из них принадлежит, будем использовать объединяющие классы и соответственно контейнеры вида cSumClassOfScheme. Объединяющий класс фиксирует систему всех совместимых между собой контейнеров и ультраконтейнеров, используемых для составляющих.

Пусть среди всех составляющих системы существует конечное подмножество, состоящее из более чем одной составляющей, каждая из которых имеет один и тот же объединяющий класс. Каждая составляющая этого подмножества характеризуется контейнерами вида cOld*. Пусть в некоторый момент времени взаимодействие системы с окружающей средой привело к введению конечного числа новых контейнеров вида cNew* для одной из составляющих рассматриваемого подмножества.

При применении предлагаемого подхода для системы контроля доступа будет обеспечена ИБ для систем реального времени. Сначала автоматически будет сгенерирована задача об обеспечении ИБ в новой системе контейнеров. При решении этой задачи:

- автоматически будут сгенерированы контейнеры cNew* для остальных составляющих рассматриваемого подмножества;
- будет поставлен вопрос о конфликтности новой системы контейнеров по доступу для обеспечения ИБ в новых условиях;
- будет выяснено, надо ли решать все задачи о заполнении управляемых контейнеров немедленно, или решение некоторых из них можно или нужно отложить.

Отметим, что при решении всех задач доступа применяются нормализованные схемы радикалов – однозначно понимаемые математические объекты. Это обеспечивает необходимую строгость при работе с проблемной областью.

Данный подход позволяет решить проблему деклассификации объекта и четко предоставляет доступ к каждому объекту в соответствии с полномочиями субъекта и допуском полномочий объекта. Также важным преимуществом этой модели будет то, что политика безопасности ИС становится универсальной: правила NWD и NRU не так сильно регламентированы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *LaPadula L., Bell D.* Secure Computer Systems: Mathematical Foundation, ESD-TR-73-278, V.1, MITRE Corporation.
2. *LaPadula L., Bell D.* Secure Computer Systems: Mathematical Foundation, ESD-TR-73-278, V.II, MITRE Corporation.
3. *Пирогов М.В.* Методика обеспечения информационно-системной безопасности сложных систем на основе математического моделирования проблемной области таких систем схемами радикалов: диссертация. – М.: Наука, 2008. – 152 с.
4. *Landwehr C.* Formal Models for Computer Security // ACM Computing Surveys. – 1984. – Vol. 13. – № 3. – 80 p.
5. *Гайдамакин Н.А.* Разграничение доступа к информации в компьютерных системах. – Изд-во Уральского ун-та, 2003. – 328 с.
6. *Лепешкин О.М., Гаппоев Р.С.* Анализ моделей мандатного разграничения доступа для систем реального времени // Научно-технические ведомости. – СПб.: СПб ГПУ, 2011. – № 3. – С. 56-64.

Статью рекомендовал к опубликованию д.т.н., профессор В.В. Копытов.

Лепешкин Олег Михайлович
Ставропольский Государственный Университет.
E-mail: lom@stavsu.ru.
г. Санкт-Петербург, проспект науки, 15\2.
Тел.: +79052851649.
К.т.н.; доцент; докторант Военной Академии Связи.

Гаппоев Расул Солтанович
E-mail: ras8w18@gmail.com.
Тел.: +79887185555.
Аспирант.

Lepeshkin Oleg Mixajlovich
Stavropol State University.
E-mail: lom@stavsu.ru.
15\2, Science Avenue, St. Petersburg, Russia.
Phone: +79052851649.
Cand. of Eng. Sc.; Assistant Professor; Doctoral Student of the Military Academy of Communication.

Gappoev Rasul Soltanovich
E-mail: ras8w18@gmail.com.
Phone: +79887185555.
Graduate Student.

УДК 004.056.5+004.8+004.93

А.Ю. Максимова, О.О. Варламов

МИВАРНАЯ ЭКСПЕРТНАЯ СИСТЕМА ДЛЯ РАСПОЗНАВАНИЯ ОБРАЗОВ НА ОСНОВЕ НЕЧЕТКОЙ КЛАССИФИКАЦИИ И МОДЕЛИРОВАНИЯ РАЗЛИЧНЫХ ПРЕДМЕТНЫХ ОБЛАСТЕЙ С АВТОМАТИЗИРОВАННЫМ РАСШИРЕНИЕМ КОНТЕКСТА

В работе показано, что для решения задач информационной безопасности целесообразно объединить возможности экспертных систем и методов распознавания образов. Целью работы является обоснование возможности совместного использования и взаимообогащения экспертных систем и распознавания образов. Первая задача работы – показать, как экспертные системы увеличивают возможности по распознаванию образов путем расширения контекста. Вторая задача – показать возможности использования методов анализа данных и распознавания образов для добавления знаний в экспертные системы. В работе получены следующие выводы. Экспертные системы позволяют обрабатывать больший контекст, что улучшает результаты распознавания. Применение методов распознавания для экспертных систем позволяет автоматизировано получать новые данные и правила в целях расширения контекста и самообучения. Показаны результаты экспериментов с миварными экспертными системами, которые подтвердили линейную вычислительную сложность миварного логического вывода и автоматического конструирования алгоритмов. Предлагается использовать нечеткий классификатор как источник правил для миварной экспертной системы. Миварные технологии позволяют на практике работать более чем с тремя миллионами продукционных правил, что кардинально увеличивает как возможности экспертных систем, так и адекватность распознавания образов в целях решения задач информационной безопасности.

Мивар; распознавание образов; информационная безопасность; экспертные системы; искусственный интеллект.