УДК 621.331.22

Защищенные структуры для систем кодирования и криптографии

В. А. Васин, канд. техн. наук; *Е. Н. Ивашов*, д-р техн. наук;
С. В. Степанчиков, канд. техн. наук
Московский институт электроники и математики НИУ ВШЭ, Москва, Россия

Рассмотрен подход к определению понятия "защищенная структура", который отличается от существующих тем, что решает проблему обеспечения безопасности систем как лежащую на стыке двух направлений: автоматизации обработки информации и общей безопасности. Это позволит объединить задачи автоматизации обработки конфиденциальной информации и разработки средств защиты в одну проблему создания защищенных информационных систем в процессе ее решения, применять методы и технологии, разработанные как в той, так и в другой области.

Ключевые слова: защищенная система обработки информации, системы кодирования и криптографии, стандарты информационной безопасности, устройство формирования изомерных квантовых точек, устройство долговременной памяти.

Многие полагают, что защищенная технологическая система — это система обработки информации, в состав которой включен тот или иной набор средств защиты. Очевидно, что это неправильный подход, так как наличие средств защиты является лишь необходимым условием и не может рассматриваться в качестве критерия защищенности системы от реальных угроз, поскольку безопасность не является абсолютной характеристикой и может рассматриваться только относительно некоторой среды, в которой действуют определенные угрозы. Поэтому считается: *защищенная система обработки информации для определенных условий эксплуатации обеспечивает безопасность (конфиденциальность и целостность) обрабатываемой информации и поддерживает свою работоспособность в условиях воздействия на нее заданного множества угроз* [1].

Взяв за основу предложенное определение, рассмотрим свойства, которыми должна обладать защищенная система.

Как и все автоматизированные (компьютерные) системы обработки информации, защищенные системы решают задачу автоматизации некоторого процесса обработки информации. Под процессом обработки информации понимаются действия, связанные с ее хранением, преобразованием и передачей. В дополнение к этому, кроме традиционных свойств, которыми обладают автоматизированные системы, — надежности, эффективности, удобства использования и так далее, защищенная система обработки информации должна обладать еще одним — свойством безопасности, которое является для нее самым главным. Наконец, поскольку проблема безопасности компьютерных систем изучается и прорабатывается уже достаточно давно, защищенная система должна соответствовать сложившимся требованиям и представлениям. Кроме того, необходимо обеспечить возможность сопоставления параметров и характеристик защищенных систем для того, чтобы их можно было сравнивать между собой.

Таким образом, под защищенной системой обработки информации предлагается понимать систему, которая обладает следующими тремя свойствами:

- осуществляет автоматизацию некоторого процесса обработки конфиденциальной информации, включая все аспекты этого процесса, связанные с обеспечением безопасности обрабатываемой информации;
- успешно противостоит угрозам безопасности, действующим в определенной среде;
- соответствует требованиям и критериям стандартов информационной безопасности.

Предложенный подход к определению понятия "защищенная система" отличается от существующих в первую очередь тем, что рассматривает проблему обеспечения безопасности систем как лежащую на стыке двух направлений: автоматизации обработки информации и общей безопасности. Это дает возможность объединить задачи автоматизации обработки конфиденциальной информации и разработки средств защиты в одну проблему создания защищенных информационных систем и процесс ее решения, применять методы и технологии, разработанные как в той, так и в другой области.

Безопасность является качественной характеристикой системы. Ее нельзя измерить в каких-либо единицах, более того, нельзя даже с однозначным результатом сравнивать безопасность двух систем: одна будет обладать лучшей защитой в одном случае, другая — в другом. Кроме того, у каждой группы специалистов, занимающихся проблемами безопасности информационных техноло-

гий, имеется свой взгляд на безопасность и средства ее достижения, а следовательно, и свое представление о том, что должна представлять собой защищенная система. Хотя любая точка зрения имеет право на существование и развитие, для того чтобы объединить усилия всех специалистов в направлении конструктивной работы над созданием защищенных систем, все-таки необходимо определить, что является целью исследований, что мы хотим получить в результате и чего в состоянии достичь.

Для ответа на эти вопросы и согласования всех точек зрения на проблему создания защищенных систем разработаны и продолжают разрабатываться стандарты информационной безопасности. Эти документы регламентируют основные понятия и концепции информационной безопасности на государственном или межгосударственном уровне. Достигнут существенный прогресс, закрепленный в новом поколении документов.

Наиболее значимыми стандартами информационной безопасности являются (в хронологическом порядке):

- "Критерии безопасности компьютерных систем Министерства обороны США" [2];
- Руководящие документы Гостехкомиссии России [3—7] (только для нашей страны);
- "Европейские критерии безопасности информационных технологий" [8];
- "Федеральные критерии безопасности информационных технологий США" [9];
- "Канадские критерии безопасности компьютерных систем" [10];
- "Единые критерии безопасности информационных технологий" [11].

Главная задача стандартов информационной безопасности — согласовать позиции и цели производителей, потребителей и аналитиков-квалификаторов в процессе создания и эксплуатации продуктов информационных технологий. Каждая из перечисленных категорий специалистов оценивает стандарты и содержащиеся в них требования и критерии по своим собственным параметрам.

Проведем сравнительный анализ существующих стандартов безопасности. Несмотря на то, что практически каждый из стандартов представляет оригинальный подход к определению понятия безопасной системы обработки информации, существует ряд понятий и концепций, используемых всеми стандартами.

В качестве обобщенных показателей, характеризующих стандарты информационной безопасности и имеющих значение для всех трех сторон, предлагается использовать универсальность, гибкость, гарантированность, реализуемость и актуальность.

Классификация рассмотренных стандартов информационной безопасности по предложенным показателям приведена в таблице.

Степень соответствия стандартов предложенным показателям определяется по следующей качественной шкале:

- ограниченное соответствие — недостаточное соответствие, при применении стандарта возникают существенные трудности;
- умеренное соответствие — минимальное соответствие, при применении стандарта в большинстве случаев существенных трудностей не возникает;
- достаточное соответствие — удовлетворительное соответствие, при применении стандарта в большинстве случаев не возникает никаких трудностей, однако эффективность предлагаемых решений не гарантируется;

Формула для работы отклонений

Стандарты безопасности	Показатели сопоставления стандартов информационной безопасности				
	Универсальность	Гибкость	Гарантированность	Реализуемость	Актуальность
Оранжевая книга (1983 г.)	Ограниченная	Ограниченная	Ограниченная	Высокая (за исключением класса А)	Умеренная
Европейские критерии (1986 г.)	Умеренная	Умеренная	Умеренная	Высокая	Умеренная
Документы ГТК (1992 г.)	Ограниченная	Ограниченная	Отсутствует	Высокая	Ограниченная
Федеральные критерии (1992 г.)	Высокая	Отличная	Достаточная	Высокая	Высокая
Канадские критерии (1993 г.)	Умеренная	Достаточная	Достаточная	Достаточная	Достаточная
Единые критерии (1999 г.)	Превосходная	Превосходная	Превосходная	Превосходная	Превосходная

• высокое соответствие — стандарт предлагает специальные механизмы и процедуры, направленные на улучшение данного показателя, применение которых позволяет получать достаточно эффективные решения;

• превосходное соответствие — улучшение данного показателя рассматривалось авторами стандарта в качестве одной из основных целей его разработки, что обеспечивает эффективность применения предложенных решений.

Представленный анализ стандартов информационной безопасности и основных тенденций их развития позволяет сделать следующие выводы.

1. Развитие стандартов привело к отказу от единой шкалы ранжирования требований и критериев, замене их множеством независимых частных показателей и введению частично упорядоченных шкал.

2. Неуклонное возрастание роли требований адекватности реализации защиты и политики безопасности свидетельствует о тенденции преобладания "качества" обеспечения защиты над ее "количеством".

3. Определение ролей производителей, потребителей и экспертов по квалификации ИТ-продуктов и разделение их функций в процессе создания защищенных систем обработки информации свидетельствует о полноправной интеграции стандартов обеспечения безопасности в сферу информационных технологий.

4. Сложившееся на основе современных стандартов разделение ролей участников процесса создания и эксплуатации защищенных систем, применение соответствующих механизмов и технологий привело к сбалансированному распределению ответственности между всеми участниками процесса.

5. Современные тенденции интеграции информационных технологий и стремление к созданию безопасного всемирного информационного пространства привели к необходимости интернационализации стандартов информационной безопасности.

Под *политикой безопасности* понимается совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое (а иногда и достаточное) условие безопасности системы. Формальное выражение политики безопасности называют *формальной моделью* политики безопасности. Формальные модели необходимы и используются достаточно широко, потому что только с их помощью можно доказать безопасность системы, опираясь при этом на объективные и неопровержимые постулаты математической теории, а также позволяют обосновать жизнеспособность системы и определяют базовые принципы ее архитектуры и используемые при ее построении технологические решения.

Основная цель создания политики безопасности информационной системы и описания ее в виде формальной модели — это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Кроме того, формальные модели безопасности позволяют решить еще целый ряд задач, возникающих в ходе проектирования, разработки и сертификации защищенных систем, поэтому их используют не только теоретики информационной безопасности, но и другие категории специалистов, участвующих в процессе создания и эксплуатации защищенных информационных систем (производители, потребители, эксперты-квалификаторы).

Среди моделей различных политик безопасности можно выделить два основных класса: дискреционные (произвольные) и мандатные (нормативные). Рассмотрим наиболее распространенные политики произвольного управления доступом, в основе которых лежат модель Харрисона—Руззо—Ульмана, модель типизованной матрицы доступа, фундаментальная нормативная модель безопасности Белла—ЛаПадулы.

Модель безопасности Харрисона—Руззо—Ульмана [12], являющаяся классической дискреционной моделью, реализует произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа.

В рамках этой модели система обработки информации представляется в виде совокупности активных сущностей — субъектов (множество S), которые осуществляют доступ к информации, пассивных сущностей — объектов (множество O), содержащих защищаемую информацию, и конечного множества прав доступа $R = \{r_1, ..., r_n\}$, означающих полномочия на выполнение соответствующих действий (например, *чтение*, *запись*, *выполнение*).

Поэтому критерий безопасности модели Харрисона—Руззо—Ульмана формулируется следующим образом.

Для заданной системы начальное состояние $Q_0 = (S_0, O_0, M_0)$ *является безопасным относительно права* **r**, *если не существует применимой к* Q_0 *последовательности команд, в результате которой право* **r** *будет занесено в ячейку матри-*

цы ***M****, в которой оно отсутствовало в состоянии* Q_0 .

Смысл данного критерия состоит в том, что для безопасной конфигурации системы субъект никогда не получит право *r* доступа к объекту, если он не имел его изначально. На первый взгляд такая формулировка кажется довольно странной, поскольку невозможность получения права *r* вроде бы влечет за собой отказ от использования команд, в которых присутствует операция **enter into** *M*[*s*, *o*], однако это не так. Дело в том, что удаление субъекта или объекта приводит к уничтожению всех прав в соответствующей строке или в столбце матрицы, но не влечет за собой уничтожение самого столбца или строки и сокращение размеров матрицы. Следовательно, если в какой-то ячейке в начальном состоянии существовало право *r*, и после удаления субъекта или объекта, к которым относилось это право, ячейка будет очищена, но впоследствии в результате создания субъекта или объекта появится вновь, и в эту ячейку с помощью соответствующей команды **enter** снова будет занесено право *r*, то это не будет означать нарушения безопасности.

Из критерия безопасности следует, что для данной модели ключевую роль играет выбор значений прав доступа и их использование в условиях команд. Хотя модель не налагает никаких ограничений на смысл прав и считает их равнозначными, те из них, которые участвуют в условиях выполнения команд, фактически представляют собой не права доступа к объектам (как, например, чтение и запись), а права управления доступом или права на осуществление модификации ячеек матрицы доступа. Таким образом, по сути дела данная модель описывает не только доступ субъектов к объектам, а распространение прав доступа от субъекта к субъекту, поскольку именно изменение содержания ячеек матрицы доступа определяет возможность выполнения команд, в том числе команд, модифицирующих саму матрицу доступа, которые потенциально могут привести к нарушению критерия безопасности.

Необходимо отметить, что с точки зрения практики построения защищенных систем модель Харрисона—Руззо—Ульмана является наиболее простой в реализации и эффективной в управлении, поскольку не требует никаких сложных алгоритмов и позволяет управлять полномочиями пользователей с точностью до операции над объектом, чем и объясняется ее распространенность среди современных систем. Кроме того, предложенный в данной модели критерий безопасности является весьма сильным в практическом плане, поскольку позволяет гарантированность недоступности определенного объекта для субъекта, которому изначально не выданы соответствующие полномочия.

Однако Харрисон, Руззо и Ульман доказали, что в общем случае не существует алгоритма, который может для произвольной системы, ее начального состояния $Q_0 = (S_0, O_0, M_0)$ и общего права *r* решить, является ли данная конфигурация безопасной. Доказательство опирается на свойства машины Тьюринга, с помощью которой моделируется последовательность переходов системы из состояния в состояние.

Для того чтобы можно было доказать указанный критерий, модель должна быть дополнена рядом ограничений [13, 14]. Не останавливаясь на математических выкладках, следует отметить, что указанная задача является разрешимой в любом из следующих случаев:

- команды α_i $(x_1,. x_k)$ являются монооперационными, т. е. состоят не более чем из одной элементарной операции;
- команды α_i $(x_1,., x_k)$ являются одноусловными и монотонными, т. е. содержат не более одного условия и не содержат операций **destroy** и **delete**;
- команды α_i $\{x_1,..., x_k)$ не содержат операций **create**.

Эти условия существенно ограничивают сферу применения модели, поскольку трудно представить себе реальную систему, в которой не будет происходить создание или удаление сущностей.

Таким образом, дискреционная модель Харрисона—Руззо—Ульмана в своей общей постановке не дает гарантий безопасности системы, однако именно она послужила основой для целого класса моделей политик безопасности, которые используются для управления доступом и контроля за распространением прав во всех современных системах.

Другая дискреционная модель, получившая название "Типизованная матрица доступа" (Type Access Matrix — TAM) [13], представляет собой развитие модели Харрисона—Руззо—Ульмана, дополненной концепцией типов, что позволяет несколько смягчить те условия, для которых возможно доказательство безопасности системы.

Формальное описание модели TAM включает следующие элементы:

- конечный набор прав доступа $R = \{r_1, ..., r_i\}$;
- конечный набор типов $T = \{t_1, ..., r_g\}$;
- конечные наборы исходных субъектов $S_0 = \{s_1, ..., s\}$ и объектов $O_0 = \{o_1, ..., o_m\}$, где $S_0 \subseteq O_0$;
- матрица *M*, содержащая права доступа субъектов к объектам, и ее начальное состояние M_0;
- конечный набор команд $C = \{\alpha_i\ (x_1,. x_k)\}$, включающий условия выполнения команд и их интерпретацию в терминах элементарных операций.

Тогда состояние системы описывается четверкой

$$Q = (S, O, t, M),$$

где S, O и M обозначают, соответственно, множество субъектов, объектов и матрицу доступа, а t: $O \to T$ — функция, ставящая в соответствие каждому объекту некоторый тип.

В работе [14] Харрисон, Руззо и Ульман показали, что критерий безопасности дискреционной модели может быть доказан для систем, в которых все команды $\alpha_i(x_1,..., x_k)$ являются одноусловными и монотонными. Строгий контроль соответствия типов позволяет смягчить требование одноусловности, заменив его ограничением на типы параметров команд, при выполнении которых происходит создание новых сущностей.

Для того чтобы сформулировать это ограничение, определим отношения между типами. Пусть $\alpha(x_1{:}t_1, x_2{:}c, \ldots, x_k{:}t_k)$ — некоторая команда ТАМ. Будем говорить, что t_i является *дочерним типом* в α, если в теле α имеет место одна из следующих элементарных операций: **create subject** x_i **of type** t_i или **create object** x_i **of type** t_i. В противном случае будем говорить, что t_i является *родительским типом* в α.

Отметим, что в одной команде тип может быть одновременно и родительским, и дочерним, например:

command **foo** ($s_1{:}u$, $s_2{:}u$, $s_3{:}w$, $o{:}b$)
create subject s_2 **of type** u;
create subject s_3 **of type** v;
end.

Здесь u является родительским типом относительно s_1 и дочерним типом относительно s_2. Кроме того, w и b являются родительскими типами, а v — дочерним типом.

Тогда можно описать взаимосвязи между различными типами с помощью графа, определяющего отношение "наследственности" между типами, устанавливаемые через операции порождения сущностей (объектов и субъектов). Такой граф называется *графом создания* и представляет собой направленный граф с множеством вершин T, в котором ребро от u к v существует тогда и только тогда, когда в системе имеется создающая команда, в которой u является родительским типом, а v — дочерним типом.

Этот граф для каждого типа позволяет определить:

сущности каких типов должны существовать в системе, чтобы в ней мог появиться объект или субъект заданного типа;

сущности каких типов могут быть порождены при участии сущностей заданного типа.

Модель монотонной типизированной матрицы доступа (МТАМ) идентична ТАМ за исключением того, что в ней отсутствуют немонотонные элементарные операции **delete**, **destroy subject** и **destroy object**.

Реализация МТАМ, состоящая из множеств объектов, субъектов, типов, матрицы прав доступа и множества команд, называется *ациклической* тогда и только тогда, когда ее граф создания не содержит циклов, в противном случае говорят, что реализация *циклическая*. Например, граф создания для приведенной выше команды **foo** содержит следующие ребра: {(u, u), (u, v), (w, u), (w, v), (b, u), (b, v)}. Реализация МТАМ, содержащая эту команду, будет циклической, поскольку тип u является для нее одновременно и родительским, и дочерним, что приводит к появлению на графе цикла (u, u).

Доказано, что критерий безопасности, предложенный Харрисоном, Руззо и Ульманом, разрешим для ациклических реализаций МТАМ и что требование одноусловности команд можно заменить требованием ацикличности графа создания [13]. Смысл этой замены состоит в том, что последовательность состояний системы должна следовать некоторому маршруту на графе создания, поскольку невозможно появление сущностей дочерних типов, если в системе отсутствуют сущности родительских типов, которые должны участвовать в их создании. Отсутствие циклов на графе создания позволяет избежать зацикливания при доказательстве критерия безопасности, так как количество путей на графе без циклов является ограниченным.

Система в модели безопасности Белла—ЛаПадулы [15], как и в модели Харрисона—Руззо—Ульмана, представляется в виде множеств субъектов S, объектов O (множество объектов включает множество субъектов, $S \subset O$) и прав доступа **read** (чтение) и **write** (запись). В мандатной модели рассматриваются только эти два вида доступа и, хотя она может быть расширена введением дополнительных прав (например, правом на добавление информации, выполнение программ и т. д.), все они будут отображаться в базовые (чтение и запись). Использование столь жесткого подхода, не позволяющего осуществлять гибкое управление доступом, объясняется тем, что в мандатной модели контролируются не операции, осуществляемые субъектом над объектом, а потоки информации, которые могут быть только двух видов: либо от субъекта к объекту (запись), либо от объекта к субъекту (чтение).

Уровни безопасности субъектов и объектов задаются с помощью функции уровня безопасности

$F{:}S \cup O \to L$, которая ставит в соответствие каждому объекту и субъекту уровень безопасности, принадлежащий множеству уровней безопасности L, на котором определена решетка Λ [16].

Решетка уровней безопасности Λ — это формальная алгебра $(L, \leq, \bullet, \otimes)$, где L — базовое множество уровней безопасности, а оператор "$\leq$" определяет частичное нестрогое отношение порядка для элементов этого множества, т. е. оператор "$\leq$" антисимметричен, транзитивен и рефлексивен.

Отношение "$\leq$" на L:

- рефлексивно, если

$$\forall\, a \in L{:}\ a \leq a;$$

- антисимметрично, если

$$\forall\, a_1, a_2, \in L{:}\ (a_1 \leq a_2 \wedge a_2 \leq a_1) \Rightarrow a_1 = a_2;$$

- транзитивно, если

$$\forall\, a_1, a_2, a_3 \in L{:}\ (a_1 \leq a_2 \wedge a_2 \leq a_3) \Rightarrow a_1 = a_3.$$

Другое свойство решетки состоит в том, что для каждой пары a_1 и a_2 элементов множества L можно указать единственный элемент *наименьшей верхней границы* и единственный элемент *наибольшей нижней границы*. Эти элементы также принадлежат L и обозначаются с помощью операторов $\bullet$ и $\otimes$, соответственно:

$$a_1 \bullet a_2 = a \Leftrightarrow a_1, a_2 \leq a \wedge \forall\, a' \in$$
$$\in L{:}\ (a' \leq a) \Rightarrow (a' \leq a_1 \vee a' \leq a_2);$$

$$a_1 \otimes a_2 = a \Leftrightarrow a \leq a_1, a_2 \wedge \forall\, a' \in$$
$$\in L{:}\ (a' \leq a_1 \wedge a' \leq a_2) \Rightarrow (a' \leq a).$$

Смысл этих определений заключается в том, что для каждой пары элементов (или множества элементов, поскольку операторы $\bullet$ и $\otimes$ транзитивны) всегда можно указать единственный элемент, ограничивающий ее сверху или снизу таким образом, что между ними и этим элементом не будет других элементов.

Функция уровня безопасности F назначает каждому субъекту и объекту некоторый уровень безопасности из L, разбивая множество сущностей системы на классы, в пределах которых их свойства с точки зрения модели безопасности являются эквивалентными. Тогда оператор "$<$" определяет направление потоков информации, т. е. если $F(A) \leq F(B)$, то информация может передаваться от элементов класса A элементам класса B.

Покажем, почему в модели Белла—ЛаПадулы для описания отношения доминирования на множестве уровней безопасности используется решетка.

Если информация может передаваться от сущностей класса A к сущностям класса B, а также от сущностей класса B к сущностям класса A, то классы A и B содержат одноуровневую информацию и с точки зрения безопасности эквивалентны одному классу (AB). Поэтому для удаления избыточных классов необходимо, чтобы отношение "$\leq$" было антисимметричным.

Если информация может передаваться от сущностей класса A сущностям класса B, а также от сущностей класса B к сущностям класса C, то очевидно, что она будет также передаваться от сущностей класса A к сущностям класса C. Таким образом, отношение "$\leq$" должно быть транзитивным.

Так как класс сущности определяет уровень безопасности содержащейся в ней информации, то все сущности одного и того же класса содержат с точки зрения безопасности одинаковую информацию. Следовательно, нет смысла запрещать потоки информации между сущностями одного и того же класса. Более того, из чисто практических соображений нужно предусмотреть возможность для сущности передавать информацию самой себе. Следовательно, отношение "$\leq$" должно быть рефлексивным.

Недостаток основной теоремы безопасности Белла—ЛаПадулы состоит в том, что ограничения, накладываемые теоремой на функцию перехода, совпадают с критериями безопасности состояния, поэтому данная теорема является избыточной по отношению к определению безопасного состояния. Кроме того, из теоремы следует только то, что все состояния, достижимые из безопасного состояния при определенных ограничениях, будут в некотором смысле безопасны, но при этом не гарантируется, что они будут достигнуты без потери свойства безопасности в процессе осуществления перехода. Поскольку не имеется никаких определенных ограничений на вид функции перехода, кроме указанных в условиях теоремы, и допускается, что уровни безопасности субъектов и объектов могут изменяться, то можно представить такую гипотетическую систему (она получила название Z-системы [17]), в которой при попытке низкоуровневого субъекта прочитать информацию из высокоуровневого объекта будет происходить понижение уровня объекта до уровня субъекта и осуществляться чтение.

Функция перехода Z-системы удовлетворяет ограничениям основной теоремы безопасности, и все состояния такой системы также являются безопасными в смысле критерия Белла—ЛаПадулы, но вместе с тем в этой системе любой пользователь сможет прочитать любой файл, что, очевидно, несовместимо с безопасностью в обычном понимании.

Следовательно, необходимо сформулировать теорему, которая бы не только констатировала безопасность всех достижимых состояний для системы, соответствующей определенным условиям, но и гарантировала бы безопасность в процессе осуществления переходов между состояниями. Для этого необходимо регламентировать изменения уровней безопасности при переходе от состояния к состоянию с помощью дополнительных правил.

Такую интерпретацию мандатной модели осуществил Мак-Лин [16], предложивший свою формулировку основной теоремы безопасности, основанную не на понятии безопасного состояния, а на понятии безопасного перехода. При таком подходе функция уровня безопасности представляется с помощью двух функций, определенных на множестве субъектов и объектов: F_s: $S \to L$ и F_o: $O \to L$.

Поскольку безопасный переход из состояния v в состояние v^* позволяет изменяться только одному элементу из v и так как этот элемент может быть изменен только способами, сохраняющими безопасность состояния, была доказана следующая теорема о свойствах безопасной системы [17].

Теорема безопасности Мак-Лина. Система безопасна в любом состоянии и в процессе переходов между ними, если ее начальное состояние является безопасным, а ее функция перехода удовлетворяет критерию Мак-Лина.

Обратное утверждение неверно. Система может быть безопасной по определению Белла—ЛаПадулы, но не иметь безопасной функции перехода, о чем свидетельствует рассмотренный пример *Z*-системы.

Такая формулировка основной теоремы безопасности предоставляет в распоряжение разработчиков защищенных систем базовый принцип их построения, в соответствии с которым для того, чтобы обеспечить безопасность системы как в любом состоянии, так и в процессе перехода между ними, необходимо реализовать для нее такую функцию перехода, которая соответствует указанным условиям.

В качестве элемента системы кодирования и криптографии выступает изомерная квантовая точка. При описании модели физического явления удобно использовать оболочечную модель ядра. В оболочечной модели ядра принимается, что энергетическая структура (уровни энергии нуклонов) ядра подобна энергетической структуре электронной оболочки атома. Сильное взаимодействие нуклонов в ядре и малый радиус этого взаимодействия позволяют рассматривать нуклоны движущимися независимо друг от друга в поле, обладающем сферически симметричным потенциалом. При этом нуклоны могут находиться в различных энергетических состояниях. Основному состоянию ядра должно соответствовать заполнение всех нижних уровней. Потеря нуклоном энергии при межнуклонных столкновениях не может перевести его в более низкое состояние, ибо все они заняты в соответствии с принципом Паули. Это приводит к тому, что длина свободного пробега нуклона в невозбужденном ядре становится больше радиуса ядра. Это означает возможность рассматривать нуклоны в рамках данной модели невзаимодействующими и несталкивающимися. Движение невзаимодействующих нуклонов в поле сферического потенциала, где орбитальный момент импульса является интегралом движения, характеризуется тем, что всем $2l+1$ возможным ориентациям вектора l соответствует одинаковый энергетический уровень. На этом уровне размещаются $2(2l+1)$ нуклонов данного типа. Таким образом, в оболочечной модели нуклоны располагаются в определенном количестве на энергетических *нуклонных оболочках.* Каждый нуклон характеризуется индивидуальной волновой функцией и индивидуальными квантовыми числами n и l.

Существуют две системы нуклонных состояний: одна для протонов, другая для нейтронов; обе системы уровней заполняются нуклонами независимо друг от друга. Ядра, имеющие только заполненные *нуклонные оболочки,* должны обладать повышенной устойчивостью (проявляющейся, например, в их большей распространенности в природе), а также должны иметь сферически симметричное распределение заряда.

Порядок заполнения нуклонных оболочек с ростом A сходен с порядком заполнения электронных оболочек с ростом Z. Ввиду сильной спин-орбитальной связи все уровни с $l \neq 0$ расщепляются на два подуровня с $j = l \pm 1/2$, заполняющихся независимо.

Предсказания оболочечной модели, в общем, соответствуют действительности. Наиболее устойчивым по сравнению с соседними ядрами являются ядра со значениями N или Z, равными **2, 8, 20, 28, 50, 82, 126** и **152**. Эти числа называются *магическими.* Распространенность в природе таких ядер наиболее велика, а квадрупольные моменты их близки к нулю. Ядра, у которых магическими числами являются и N и Z, называются *дважды магическими.* Эти ядра ($_2He^4$, $_8O^{16}$, $_{20}Ca^{40}$, $_{32}Pb^{208}$) отличаются особой устойчивостью, проявляющейся, в частности, в том, что они являются наиболее

распространенными в природе изотопами этих элементов.

Гамма-излучением называется жесткое электромагнитное излучение, энергия которого высвобождается при переходах ядер из возбужденного в основное или в менее возбужденное состояние, а также при ядерных реакциях.

В первом случае энергия γ-квантов равна разности энергий конечного и начального уровней ядра. В каждом акте перехода ядро излучает один γ-квант. В связи с дискретностью энергетических уровней ядра гамма-излучение имеет линейчатый спектр. Частоты γ-квантов связаны с разностью энергий условием частот Бора.

При испускании ядром γ-кванта само ядро вследствие закона сохранения импульса приобретает противоположно направленный импульс *(отдача)*. Если ядра, испускающие γ-кванты, находятся в твердом теле, то спектр гамма-лучей состоит из двух компонент:

компоненты с естественной шириной гамма-линии Γ, определяемой временем жизни ядер в данном возбужденном состоянии, с энергией E;

компоненты с шириной линии $\Gamma_R \sim E\frac{\overline{u}}{c} \gg \Gamma$,

где $\overline{u}$ — средняя квадратичная скорость теплового движения гамма-радиоактивных ядер в твердом теле; эта компонента имеет энергию, смещенную относительно значения E на величину энергии отдачи $R = \frac{E^2}{2M_0c^2}$, где M_0 — масса излучающего ядра (если считать его свободным и движущимся со скоростью $\overline{u \ll c}$).

В результате линии гамма-излучения и поглощения (той же линии) сильно размываются и, кроме того, сдвинуты по энергии друг относительно друга на величину ~2R. Ввиду того, что для гамма-излучения R в общем не мало по сравнению с E, *явление резонансного поглощения гамма-лучей* ($E_{изл} = E_{погл}$ или $\nu_{изл} = \nu_{погл}$) обычно практически не наблюдается.

При определенных условиях удается добиться того, что излучаемый гамма-квант передает импульс не одному излучающему ядру, а всему кристаллу в целом. В результате излучаемой линии соответствует энергия отдачи $R \approx 0$ (M — велико) и $\Gamma_R \approx \Gamma$, т. е. ширина линий приближается к естественной, а сдвиг по энергии практически исчезает. Одним из условий четкого проявления эффекта Мессбауэра является условие $R \le 2k\Theta_D$, где Θ_D — дебаевская температура кристалла, k — постоянная Больцмана. При $R << 2k\Theta_D$ гамма-переходы "без отдачи" можно наблюдать уже при комнатной температуре.

Варианты технических устройств для получения элементов систем кодирования и криптографии

Устройство формирования изомерных квантовых точек

В основу разработки положена задача создания наногетероструктур, способных сохранять возбужденное состояние.

Устройство формирования изомерных квантовых точек 1 для систем (рис. 1) долговременной памяти на подложке 2 содержит зонд 3, закрепленный на пьезоприводе 4 [18]. Подложка электрически связана (5) с зондом и установлена в ванной 6 с соляным раствором вещества 7, ядра которого обладают ядерной изомерией.

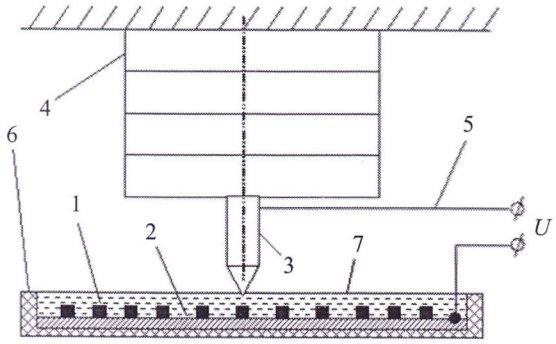

Рис. 1. Устройство формирования изомерных квантовых точек

При подаче рабочего напряжения в соляном растворе начинает протекать процесс электролиза, обеспечивающего формирование квантовых точек на подложке.

Применение устройства позволяет создать наногетероструктуры, способные сохранять возбужденные состояния в течение нескольких лет.

Устройство долговременной памяти

В основу разработки положена задача повышения плотности записи информации на записывающей матрице.

Устройство долговременной памяти (рис. 2) содержит записывающую матрицу 1, излучатель электромагнитных волн 2, вещество-приемник 3, расположенное на матрице [19]. Вещество-приемник выполнено из радиоактивного материала с изомерными ядрами. Излучатель электромагнитных волн выполнен в виде источника 4 гамма-лучей — фотонов большой энергии. В качестве

излучателя гамма-лучей — фотонов большой энергии — использован лазерный генератор 5 с возможностью перевода изомерных ядер вещества-приемника в возбужденное состояние на период до нескольких лет. Записывающая матрица связана с трехкоординатным приводом 6, установленным на неподвижном основании 7.

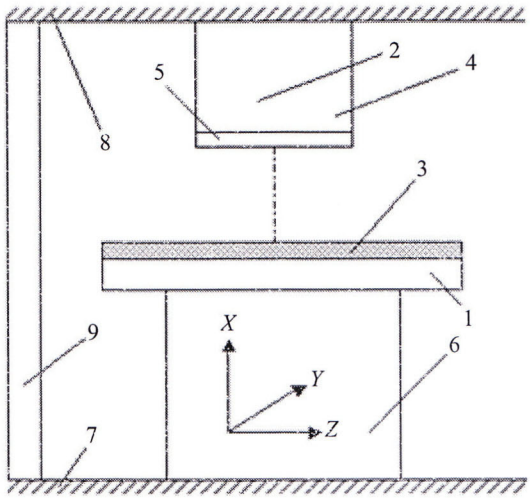

Рис. 2. Устройство долговременной памяти

Лазерный генератор также закреплен на втором неподвижном основании 8, причем первое и второе основания 7, 8 связаны между собой жесткой планкой 9.

Источник гамма-лучей (фотонов большой энергии) — лазерный генератор — воздействует на изомерные ядра вещества-приемника, переводя их в возбужденное состояние, в котором они могут находиться несколько лет. Одно изомерное возбужденное ядро соответствует одному биту информации. Таким образом, плотность записи информации резко повышается.

Применение устройства долговременной памяти позволяет повысить плотность записи информации на три порядка, при котором размер одного бита информации составляет не более 1 нм.

Литература

1. *Зегжда Д. П., Ивашко А. М.* Основы безопасности информационных систем. — М.: Горячая линия — Телеком, 2000.
2. Trusted Computer System Evaluation Criteria. Us Department of Defense 5200.28-STD, 1993.
3. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники от несанкционированного доступа к информации. — М., 1992.
4. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. — М., 1992.
5. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. — М., 1992.
6. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. — М., 1992.
7. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. — М., 1992.
8. Information Technology Security Evaluation Criteria. Harmonized Criteria of France-Germany-Netherlands-United Kingdom. — Department of Trade and Industry, London, 1991.
9. Federal Criteria for Information Technology Security// National institute of Standards and Technology & National Security Agency. Version 1.0, December 1992.
10. Canadian Trusted Computer Product Evaluation Criteria// Canadian System Security Centre Communication Security Establishment, Government of Canada. Version 3.0e. January 1993.
11. Common Criteria for Information Technology Security Evaluation// National Institute of Standards and Technology & National Security Agency (USA), Communication Security Establishment (Canada), Communication-Electronics Security Group (United Kingdom), Bundesamt fur Sichereit in der Informationstechnik (Germany), Service Central de la Securite des Systemes d'Information (France), National Communications Security Agency (Netherlands). Version 2.1, August 1999.
12. *Harrison M., Ruzzo W., Uhlman J.* Protection operating systems // Communications of the ACM, 1976.
13. *Ravi S.* Sandhu The Typed Acess Matrix Model// Proceedings of IEEE Symposium on Security and Privacy. — Oakland, California, May 4—6, 1992. P. 122—136.
14. *Harrison M., Ruzzo W.* Monotonic protection systems// Foundation of secure computation, 1978.
15. *Leonard J.* LaPadula and D. Elliot Bell. Secure Computer Systems: A Mathematical Model// MITRE Corporation Technical Report, 2547, V. II, 31 May 1973.
16. Ciaran Bryce Lattice-Based Enforcement of Access Control Policies// Arbeitspapiere der GMD (Research Report), N. 1020, August 1996.
17. *John McLean.* The Specification and Modeling of Computer Security// Computer, 23(1):9—16, January 1990.
18. *Ивашов Е. Н., Козанов Т. Т., Мазур Н. В. и др.* Устройство формирования квантовых точек. Патент 66607 РФ. Опубл. 10.09.2007. Бюл. № 25.
19. *Ивашов Е. Н., Козанов Т. Т., Мазур Н. В. и др.* Устройство долговременной памяти. Патент 66609 РФ. Опубл. 10.09.2007. Бюл. № 25.

Protected structure for systems of coding and cryptography

V. A. Vasin, E. N. Ivashov, S. V. Stepanchikov
Moscow Institute of Electronics and Mathematics NRU Higher School of Economics, Russia

In this paper, the approach to the definition of "protected structure", which is different from those existing in the first place that addresses the issue of security systems, such as lying at the intersection of two areas: the automation of information processing and overall safety. This allows you to combine the tasks of automation for handling confidential information and to develop remedies for a problem of secure information systems in the course of its decision to apply the methods and technologies developed in one and in another area.

Keywords: secure system of information processing, coding system and cryptography, information security standards, formation of isomeric unit of quantum dots, non-volatile memory device.

Васин Владимир Анатольевич, старший научный сотрудник.
Ивашов Евгений Николаевич, профессор.
Степанчиков Сергей Валентинович, доцент.
E-mail: vacuumwa@list.ru, ienmiem@mail.ru

Статья поступила в редакцию в июле 2012 г.

* * *