УДК 004.052

В.Г. Миронова, А.А. Шелупанов, Н.Т. Югов

Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях

Рассмотрена модель Take-Grant, реализующая дискреционную политику разграничения прав доступа на примере модели «Система контроля и управления доступом» на охраняемую территорию. Модель Take-Grant является моделью, которая реализует дискреционную политику безопасности и предоставляет возможность анализировать и проверять безопасность состояния систем.

Ключевые слова: политика безопасности, модель Take-Grant.

Жизнь современного общества немыслима без повсеместного применения информационных технологий. В настоящее время компьютерные системы и телекоммуникации определяют надежность систем обороны и безопасности страны, реализуют современные информационные технологии, обеспечивая обработку и хранение информации, автоматизируют технологические процессы. Массовое использование компьютерных систем, которое позволило решить проблему автоматизации процессов производства, обработки и хранения информации, сделало уязвимым эти процессы, в результате чего появилась новая проблема – проблема информационной безопасности. Одним из решений проблемы информационной безопасности является создание политики безопасности.

Под политикой безопасности понимается совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое условие безопасности системы [1].

Существует два типа политик безопасности: мандатная и дискреционная.

Целью мандатной политики безопасности является предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа.

Основу мандатной политики безопасности составляет мандатное управление доступом, которое подразумевает, что:

– все субъекты и объекты системы должны быть однозначно идентифицированы;

– задан линейно упорядоченный набор меток секретности;

– каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации;

– каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему в информационной системе (ИС) [2].

В настоящее время широко используется дискреционная политика безопасности, к достоинствам которой можно отнести относительно простую реализацию механизмов защиты информации в информационных системах (ИС).

Основой дискреционной политики безопасности является дискреционное управление доступом, которое определяется двумя свойствами:

– все субъекты и объекты должны быть идентифицированы;

– права доступа субъектов к объекту ИС определяются на основании некоторого внешнего по отношению к системе правила [2].

В случае использования дискреционной политики безопасности возникает необходимость определения правил распространения прав доступа и анализа их влияния на безопасность ИС.

Модель Take-Grant является моделью, которая реализует дискреционную политику безопасности и предоставляет возможность анализировать и проверять безопасность состояния ИС.

В модели Take-Grant в качестве основных элементов используются граф доступов и правила его преобразования. Формально описание модели Take-Grant выглядит следующим образом:

1. Множество объектов – $\mathbf{O}$, где $o_j \in \mathbf{O}$, $\mathbf{O} = \{o_1, o_2, \ldots, o_j\}$, $j \in \mathbf{N}$;

2. Множество субъектов – $\mathbf{S}$, где $s_n \in \mathbf{S}$, $\mathbf{S} = \{s_1, s_2, \ldots, s_n\}$, $n \in \mathbf{N}$;

3. Множество активных субъектов – $\mathbf{S} \subseteq \mathbf{O}$;

4. Множество прав доступа **R**, где $r_i \in \mathbf{R}$, $\mathbf{R} = \{r_1, r_2, \ldots, r_j\} \cup \{t, g\}$, где t (*take)* – право брать права доступа, g(grant) – права давать права доступа;

5. Конечный помеченный ориентированный граф **G** без петель, представляющий текущие доступы в системе, **G** = (**S**, **O**, **E**), где элементы множества $\mathbf{E} \subseteq \mathbf{O} \times \mathbf{O} \times \mathbf{R}$ представляют дуги графа **G**, помеченные непустыми подмножествами из множества прав доступа **R**.

В качестве модели безопасности ИС рассмотрим модель типа «Система контроля и управления доступом (СКУД)».

Пусть для СКУД имеется множество субъектов **S**, $s_n \in \mathbf{S}$, $\mathbf{S} = \{s_1, s_2, \ldots, s_n\}$, $n \in \mathbf{N}$, где под субъектами понимаются:

− работники организации;

− бюро пропусков;

− программа «СКУД», отвечающая за работу турникета и идентификацию субъектов доступа по предъявленным пропускам;

− контролер (часовой);

− прочий персонал ИС, который обладает пропуском на охраняемую территорию.

Объектом o_1, $o_j \in \mathbf{O}$, $\mathbf{O} = \{o_1, o_2, \ldots, o_j\}$, где $j \in \mathbf{N}$, обозначим охраняемую территорию.

Права доступа на охраняемую территорию (наличие пропуска) субъекта s_n обозначим как r_1, $r_1 \in \mathbf{R}$, $\mathbf{R} = \{r_1, r_2, \ldots, r_j\} \cup \{t, g\}$.

Согласно аксиомам, представленным в [2], в модели типа «СКУД» активными компонентами (субъектами), выполняющими контроль операций субъектов над объектом, будет являться программа «СКУД» и(или) контролер (часовой).

Монитор обращения (МО) в модели типа «СКУД» – субъект s_n, $s_n \in \mathbf{S}$, $\mathbf{S} = \{s_1, s_2, \ldots, s_n\}$, $n \in \mathbf{N}$, который в модели представлен программой «СКУД» (рис. 1).

Доступом субъектов для множества субъектов **S**, $s_n \in \mathbf{S}$, $\mathbf{S} = \{s_1, s_2, \ldots, s_n\}$, $n \in \mathbf{N}$ – общее количество субъектов, имеющих право доступа к объекту o_1, будем называть порождение потока информации между объектом o_1 и множеством субъектов **S**.

Получив запрос на доступ от субъекта **S** к объекту o (при предъявлении пропуска работником организации), монитор безопасности обращений анализирует базу правил (базу данных субъектов, имеющих право доступа в охраняемую зону), соответствующую установленной в системе политике безопасности, и либо разрешает проход на охраняемую территорию, либо запрещает.

Монитор безопасности обращений удовлетворяет следующим свойствам:

1. Ни один запрос на доступ субъекта к объекту не должен выполняться в обход МБО.

2. Работа МБО должна быть защищена от постороннего вмешательства.

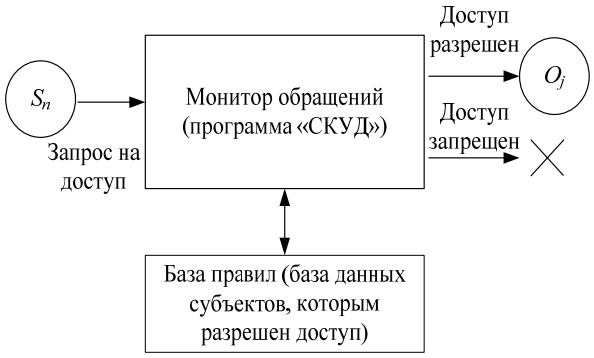

Рис. 1. Монитор обращений в модели «СКУД»

3. Представление МБО должно быть достаточно простым для возможности верификации корректности его работы.

Монитор безопасности объектов (МБО) – представлен субъектом из субъектов **S** и в модели является программой «СКУД» и(или) контролером (часовым).

Под монитором порождения субъектов (МПС) в модели типа «СКУД» будем понимать субъект из множества **S**, который будет представлен как бюро пропусков.

Монитор безопасности субъектов (МБС) в модели типа «СКУД» – субъект из **S**, который представлен как бюро пропусков.

На рис. 2 показана схема защищенной компьютерной системы.

В случае использования дискреционной политики безопасности основной функцией МБО является предоставление доступа к объекту только для санкционированных относительно данного объекта субъектов. При этом перед МБО стоит неразрешимая задача – проверить, приведут ли его действия к нарушению безопасности объекта или нет. Модель Take-Grant предоставляет алгоритм для проверки безопасности ИС.

Согласно [3] субъект **M** – множество нарушителей информационной безопасности в модели типа «СКУД» может получить право доступа к объекту доступа o_1 (пропуск на охраняемую территорию), если существует субъект s_1, имеющий право доступа (пропуск на охраняемую территорию), такой, что субъекты m_1 и s_1 связаны произвольно ориентированной дугой, содержащей хотя бы одно из прав t (*take*) или g (*grant*).

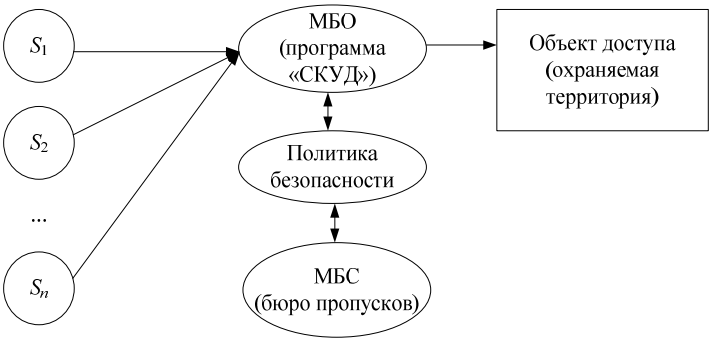

Рис. 2. Схема защищенной компьютерной системы

На рис. 3 показан граф **G** предоставления прав доступа в модели типа «СКУД» в правилах модели Take-Grant, где **S** – множество субъектов, **M** – множество субъектов-нарушителей, $m \in \mathbf{M}$, $\mathbf{M} = \{m_1, m_2, \ldots, m_k\}$, где $k \in \mathbf{N}$, o_1 – объект доступа (охраняемая территория); **R** – множество прав доступа к объекту o_1 и m_1, s_1, o_1 – различные вершины графа **G**. Использовано правило классической модели Take-Grant «Давать» – *grant* (r_1, s_1, m_1, o_1). Таким образом, нарушитель m_1 получил право доступа на охраняемую территорию.

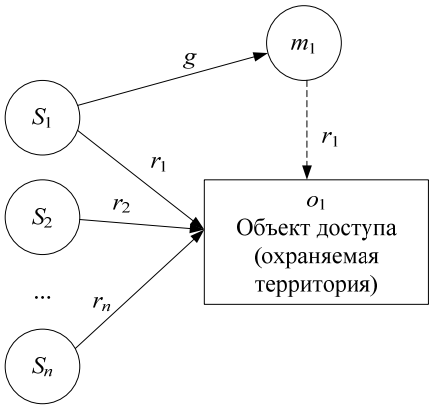

Рис. 3. Граф предоставления прав доступа в модели типа «СКУД»

Приведем пример реализации дискреционной политики разграничения прав доступа. Пусть в организации ведется обработка конфиденциальной информации в ИС. ИС имеет локальную структуру, в состав которой входят рабочие места пользователей ИС и сервер ИС. Доступ к серверу с рабочих мест пользователей осуществляется в терминальном режиме. Сервер ИС расположен в отдельном помещении, которое определено как охраняемая зона (рис. 4). Вход в это помещение разрешен только двум сотрудникам, выполняющим обязанности администраторов ИС, согласно приказу директора организации. Контроль доступа в помещение ведется с помощью системы контроля доступа. Администраторы ИС, которым разрешен доступ на охраняемую территорию, обладают пропусками для входа.

Для того чтобы пройти в помещение, в котором установлен сервер, администратору необходимо воспользоваться системой контроля доступа и предъявить пропуск.

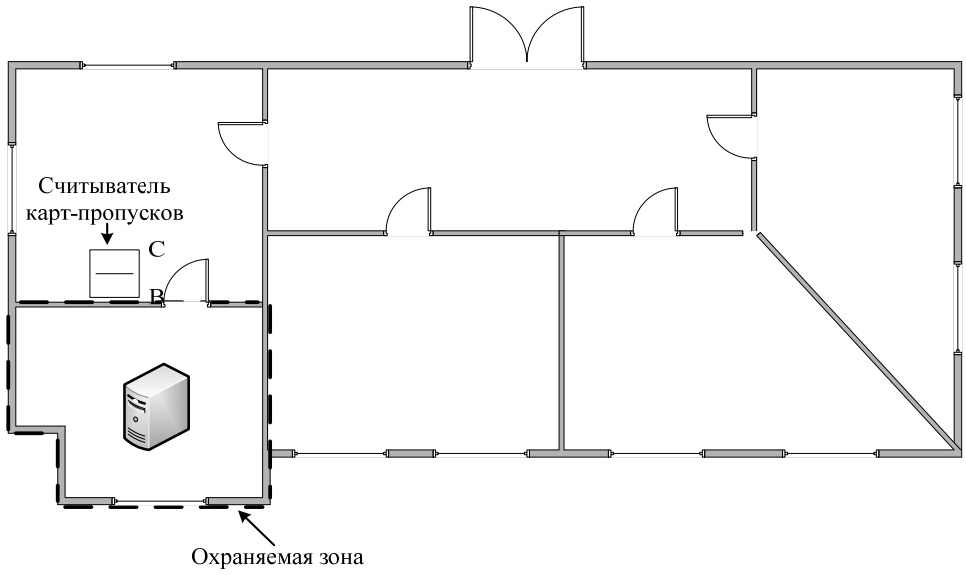

Рис. 4. Схема охраняемой территории

На рис. 5 показана схема получения пропуска для входа в помещение, в котором установлен сервер ИС.

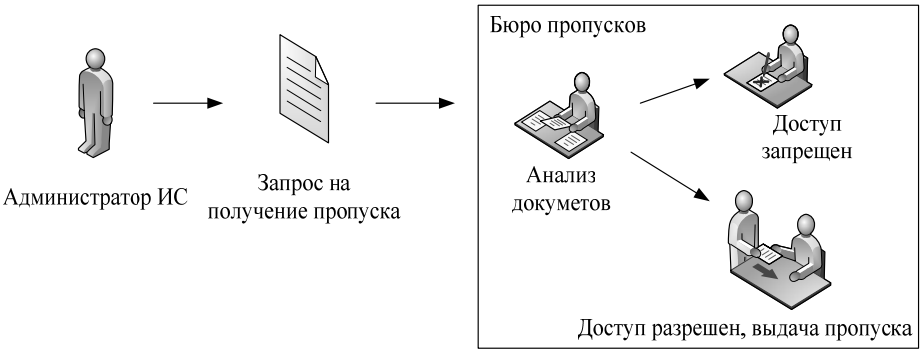

Рис. 5. Схема выдачи пропуска администратору ИС

На рис. 6 показана схема санкционированного прохода администратора ИС в помещение, в котором установлен сервер.

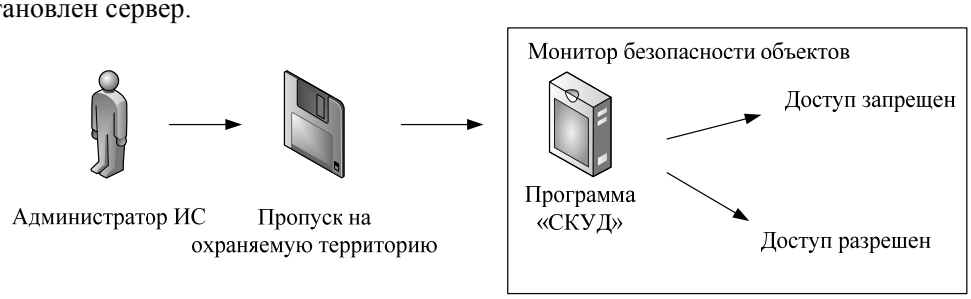

Рис. 6. Схема санкционированного прохода администратора ИС в помещение, в котором установлен сервер

На рис. 7 представлена схема несанкционированного прохода нарушителя в помещение, в котором установлен сервер. Получение прав доступа в помещение (пропуска) возможно путем передачи пропуска одним из администраторов ИС нарушителю.

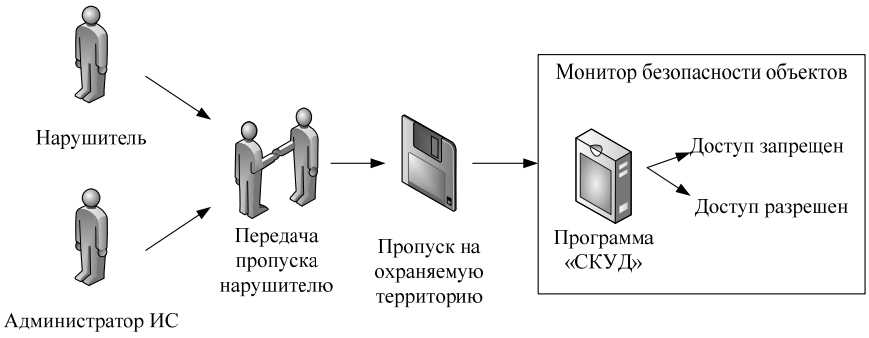

Рис. 7. Схема несанкционированного прохода нарушителя на охраняемую территорию

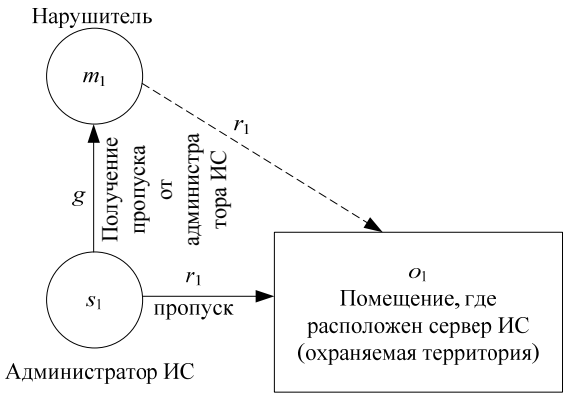

Рис. 8. Модель Take-Grant

На рис. 8 представлена схема модели Take-Grant, которая позволяет отследить возможную угрозу передачи прав доступа в охраняемую зону (пропуск в помещение, в котором установлен сервер ИС).

Одна из важных проблем, которые возникают при использовании дискреционной политики безопасности, – это проблема контроля распространения прав доступа. Отследить распространение прав доступа и максимально их ограничить позволяет использование модели Take-Grant.

Литература

1. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М.: Горячая линия – Телеком, 2000. – 452 с.

2. Девянин П.Н. Модели безопасности компьютерных систем: учеб. пособие для студ. высш. учеб. заведений. – М.: Изд. центр «Академия», 2005. – 144 с.

3. Грушо А.А. Теоретические основы защиты информации / А.А Грушо., Е.Е. Тимонина. – М.: Изд-во агентства «Яхтсмен», 1996. – 187 с.

4. Миронова В.Г. Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности / В.Г. Миронова, А.А. Шелупанов // Докл. Том. гос. ун-та систем управления и радиоэлектроники. – 2010. – № 2(22), ч. 1. – С. 257–259.

Миронова Валентина Григорьевна
Аспирант каф. информационной безопасности электронно-вычислительных систем ТУСУРа
Тел.: 8-923-415-16-08
Эл. почта: mvg@security.tomsk.ru

Шелупанов Александр Александрович
Д-р техн. наук, профессор, проректор по научной работе ТУСУРа
Эл. почта: saa@udcs.ru

Югов Николай Тихонович
Д-р техн. наук, профессор каф. высшей математики ТУСУРа
Эл. почта: office@udcs.ru

Mironova V.G., Shelupanov A.A., Yugov N.T.

Implementation of Take-Grant model as a representation of user access rights differentiation system in the building

A Take-Grant model implements the discretionary policy of access right differentiation through the example of «System Access Control» model to the protected area. Take-Grant model is a model that implements the discretionary security policy and gives the opportunity to analyze and verify the security of the systems.
Keywords: security policy, Take-Grant model.
