Модели основных типов политики безопасности

Политика 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. Формальное выражение политики безопасности называют моделью безопасности.

Основная цель создания политики безопасности 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

Политика безопасности

Информационная безопасность - сравнительно молодая, быстро развивающаяся область информационных технологий. Под информационной безопасностью будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации - это комплекс мероприятий, направленных на обеспечение информационной безопасности. Угрозы информационной безопасности - это оборотная сторона использования информационных технологий.

Модели безопасности

Основную роль в методе формальной разработки системы играет так называемая *модель безопасности (модель управления доступом, модель политики безопасности)*. Целью этой модели является выражение сути требований по безопасности к данной системе. Она определяет потоки информации, разрешенные в системе, и правила управления доступом к информации.

Модель позволяет провести анализ свойств системы, но не накладывает ограничений на реализацию тех или иных механизмов защиты. Так как она является формальной, возможно осуществить доказательство различных свойств безопасности системы.

Хорошая модель безопасности обладает свойствами абстрактности, простоты и адекватности моделируемой системе.

Модели безопасности

- *Доступ к информации* — ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации
- *Объект доступа* — единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа
- *Субъект доступа* — лицо или процесс, действия которого регламентируются правилами разграничения доступа.
- *Правила разграничения доступа* — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

Модели безопасности

Модель распространения прав доступа.

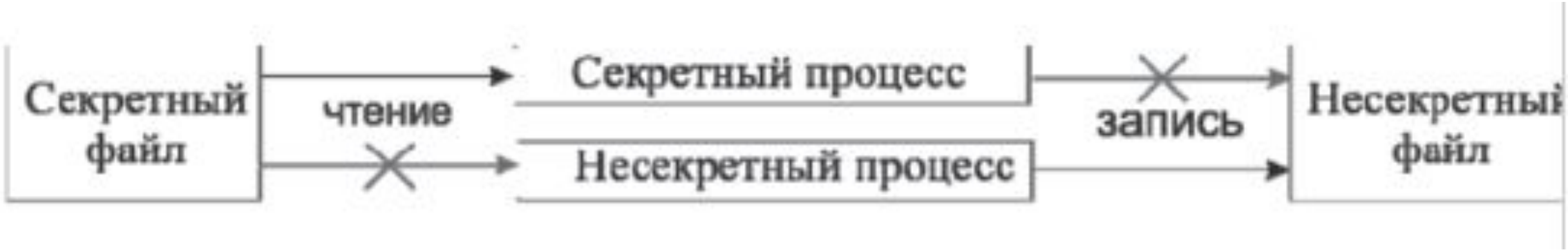
Модель матрицы доступов Харрисона –Рузо – Ульмана.

Модель системы безопасности Белла – ЛаПадулы.

Модель ролевого разграничения доступа.

Модель безопасности белла-ЛаПадулы

Эта модель в основном известна двумя основными правилами безопасности: одно относится к чтению, а другое – к записи данных.



Пусть в системе имеются данные (файлы) двух видов: *секретные* и *несекретные,* а пользователи это системы также относятся к двум категориям: с уровнем допуска к несекретным данным (несекретные) и с уровнем допуска к секретным данным (секретные).

- 1. Свойство простой безопасности: несекретный пользователь (или процесс, запущенный от его имени) не может читать данные из секретного файла.

Пусть в системе имеются данные (файлы) двух видов: *секретные* и *несекретные,* а пользователи этой системы также относятся к двум категориям: с уровнем допуска к несекретным данным (несекретные) и с уровнем допуска к секретным данным (секретные).

Пользователь с уровнем доступа к секретным данным не может записывать данные в несекретный файл. Если пользователь с уровнем доступа к секретным данным скопирует эти данные в обычный файл (по ошибке или злому умыслу), они станут доступны любому «несекретному» пользователю. Кроме того, в системе могут быть установлены ограничения на операции с секретными файлами (например, запрет копировать эти файлы на другой компьютер, отправлять их по электронной почте и т. д.). Второе правило безопасности гарантирует, что эти файлы (или даже просто содержащиеся в них данные) никогда не станут несекретными и не «обойдут» эти ограничения. Таким образом, вирус, например, не сможет похитить конфиденциальные данные.

Модель безопасности белла-ЛаПадулы

Общее правило звучит так: пользователи могут читать только документы, уровень секретности которых не превышает их допуска, и не могут создавать документы ниже уровня своего допуска. То есть теоретически пользователи могут создавать документы, прочесть которые они не имеют права.

Модель Белла-ЛаПадулы стала первой значительной моделью политики безопасности, применимой для компьютеров, и до сих пор в измененном виде применяется в военной отрасли. Модель полностью формализована математически.

Основой модели является конфиденциальность.

Модель матрицы доступов Харрисона –Рузо – Ульмана.

Модель Харрисона - Руззо - Ульмана (Harrison, Ruzo Ullman, 1976). используется для анализа систем защиты, реализующих дискреционную политику безопасности.

Это частный случай реализации модели машины состояний. Состояния безопасности системы представлены в виде таблицы, содержащей по одной строке для каждого субъекта системы и по одной колонке для каждого субъекта и объекта. Каждое пересечение в массиве определяет режим доступа данного субъекта к каждому объекту или другому субъекту системы.

Модель матрицы доступов Харрисона –Рузо – Ульман

При использовании матричной модели доступа должны быть определены множества субъектов S, объектов O и прав доступа R.

Субъекты	Объекты				
	o_1	0_2	Os		o_v
Si	R,W,D	R			R,W
s_2	R	—	—		R
Sn	R,W	R	R		R,W

Примечание:
R— право чтения;
W — право записи;
D — право удаления.

Для модели Харрисона-Рузо-Ульмана были доказаны следующие утверждения:

- Существует алгоритм, который проверяет, является ли исходное состояние монооперационной системы безопасным для данного права г.
- Задача проверки безопасности произвольных систем алгоритмически неразрешима.

Модель Take-Grant

Модель TAKE-GRANT, имеющая важное теоретическое значение в исследовании процессов распространения прав доступа в системах, основанных на политике дискреционного доступа, была представлена Джонсом, Липтоном и Шнайдером в 1976 г.

Take + Grant

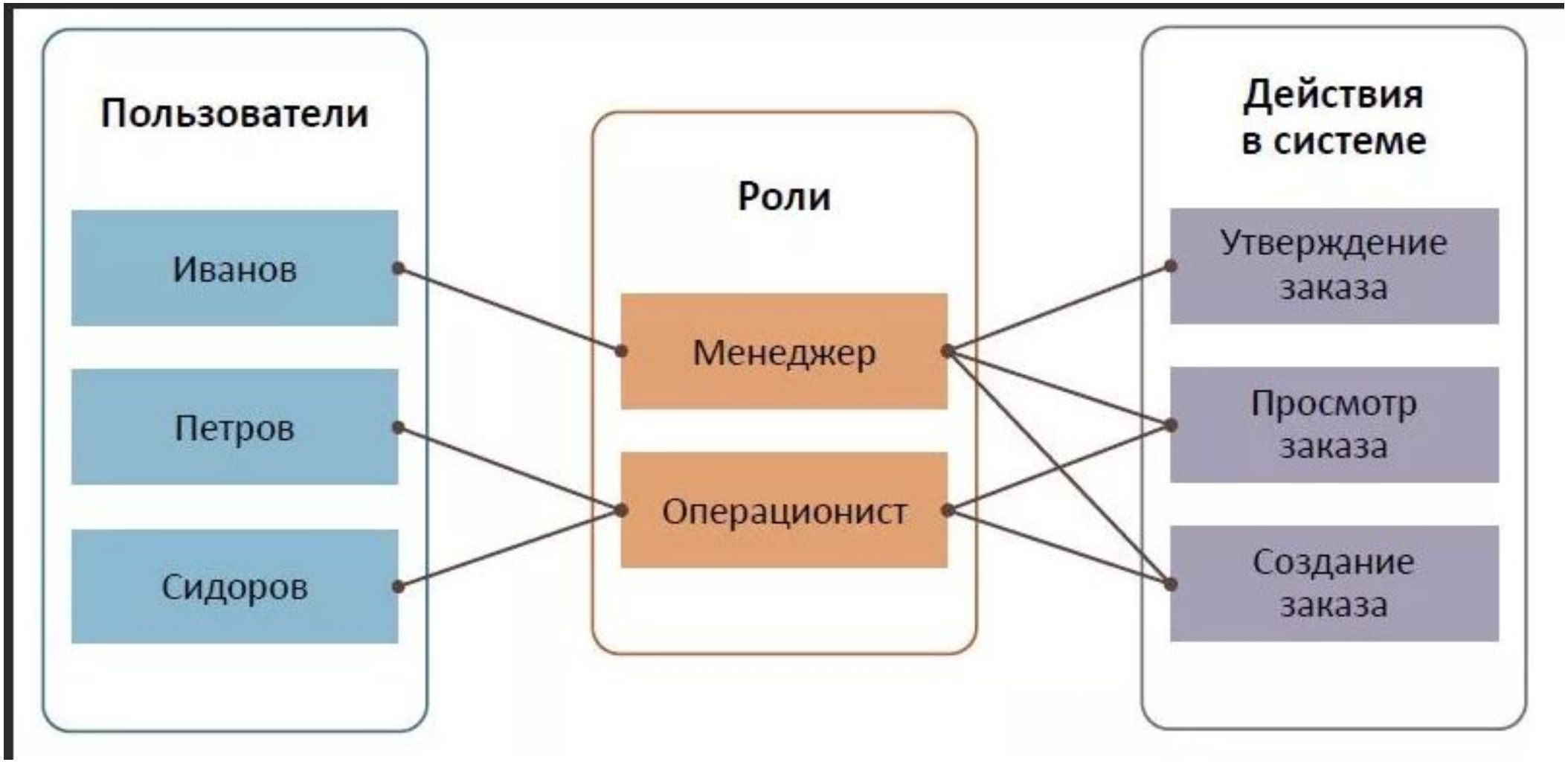
Брать Давать

Модель Take-Grant

Модель распространения прав доступа Take-Grant, предложенная в 1976 г., используется для анализа систем дискреционного разграничения доступа, в первую очередь для анализа путей распространения прав доступа в таких системах. В качестве основных элементов модели используются граф доступов и правила его преобразования.

Цель модели - дать ответ на вопрос о возможности получения прав доступа субъектом системы на объект в состоянии, описываемом графом доступов. В настоящее время модель Take-Grant получила продолжение как расширенная модель Take-Grant, в которой рассматриваются пути возникновения информационных потоков в системах с дискреционным разграничением доступа.

РОЛЕВАЯ МОДЕЛЬ ДОСТУПА (RBAC)



Модели разграничения доступа

Разграничение доступа — совокупность правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы. Также данные правила называют *правами доступа* или *политиками безопасности*. Существуют две основные модели разграничения доступа:

- мандатное разграничение доступа;
- дискреционное (избирательное) разграничение доступа.

Мандатное разграничение доступа

В мандатной модели обычные пользователи лишены возможности управлять настройками политик безопасности. Например, возможность доступа к тому или иному объекту определяется уровнем секретности объекта и уровнем доступа пользователя, которые жестко заданы для каждого пользователя и объекта. Данная модель обладает невысокой гибкостью и высокой трудоемкостью настройки политик безопасности, но при этом позволяет достичь высокого уровня управляемости безопасностью.

Дискреционное разграничение доступа

Дискреционное (избирательное, контролируемое) разграничение доступа — управление доступом субъектов к объектам базируется на том, что пользователи в том или ином объеме могут управлять настройками политик безопасности. Наиболее популярной реализацией дискреционной модели является модель, которая реализует ограничение доступа к файлам и объектам межпроцессной коммуникации в обычных пользовательских представителях семейств операционных систем Unix и Windows. В этих реализациях пользователь может произвольно изменить права доступа к файлу, который он создал, например, сделать его общедоступным.