10 Назовите государственные органы, обеспечивающие безопасность информационных технологий, и решаемые ими задачи.

Органы государственной безопасности являются составной частью системы обеспечения национальной безопасности Республики Беларусь. Руководство деятельностью органов государственной безопасности осуществляют Президент Республики Беларусь и Совет Министров Республики Беларусь в пределах полномочий, делегированных ему Президентом Республики Беларусь. Органы государственной безопасности образуют единую централизованную систему, в которую входят: Комитет государственной безопасности Республики Беларусь; управления Комитета государственной безопасности Республики Беларусь по областям (территориальные органы); управление военной контрразведки Комитета государственной безопасности Республики Беларусь. Управления Комитета государственной безопасности Республики Беларусь по областям и управление военной контрразведки Комитета государственной безопасности Республики Беларусь находятся в подчинении Комитета государственной безопасности Республики Беларусь. **Комитет государственной безопасности Республики Беларусь** — республиканский орган государственного управления, проводящий в пределах своей компетенции государственную политику в сфере обеспечения национальной безопасности Республики Беларусь, осуществляющий регулирование и управление в сфере обеспечения безопасности личности, общества и Государственное регулирование и управление в области информации, информатизации и защиты информации осуществляются Президентом Республики Беларусь, Советом Министров Республики Беларусь, Национальной академией наук Беларуси, **Президент Республики** Беларусь в соответствии с Конституцией Республики Беларусь, настоящим Законом и иными законодательными актами Республики Беларусь определяет единую государственную политику и осуществляет иное государственное регулирование в области информации, информатизации и защиты информации.

**Совет Министров Республи**ки Беларусь в области информации, информатизации и защиты информации:обеспечивает проведение единой государственной политики;координирует, направляет и контролирует работу республиканских органов государственного управления и иных государственных организаций, подчиненных Правительству Республики Беларусь;утверждает государственные программы, если иное не предусмотрено законодательными актами Республики Беларусь, и обеспечивает их реализацию; **Национальная академия наук Беларуси**: осуществляет научно-методическое обеспечение развития информатизации, реализации государственных программ;участвует в разработке проектов нормативных правовых актов;осуществляет иные полномочия в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

**Оперативно-аналитический центр при Президенте Республики Беларусь** в области защиты информации:координирует деятельность по технической защите информации;осуществляет в пределах своих полномочий контроль за деятельностью по обеспечению технической защиты информации;участвует в разработке проектов нормативных правовых актов в области технической защиты информации; **Министерство связи и информатизации Республики Беларусь** в области информатизации:реализует единую государственную политику;разрабатывает и реализует государственные программы;участвует в разработке проектов нормативных правовых актов;координирует работу по формированию и государственной регистрации информационных ресурсов; **Иные государственные органы** в пределах своих полномочий в области информации, информатизации и защиты информации:участвуют в реализации единой государственной политики;формируют и используют информационные ресурсы;создают и развивают информационные системы и информационные сети, обеспечивают их совместимость и взаимодействие в информационном пространстве Республики Беларусь; **Совет безопасности Республики Беларусь**является высшим коллегиальным координационно-политическим органом, создаваемым в целях определения военной политики республики в области безопасности, стратегии, принципов военного строительства, обеспечения гарантированной защиты суверенитета, оборонного потенциала республики, ее экологического состояния, прав и свобод граждан.

48 Опишите типы политики безопасности.

**В программных системах также широко используют два типа политики безопасности.**

***ДИСКРЕЦИОННАЯ (дискретная) политика безопасности***– *имеет в основе дискреционное*(действующее по усмотрению чего (кого)-либо) *управление доступом*: *DAC*– *Discretionary access control*.

**Это управление определяется *свойствами*:**

*а) все субъекты и объекты должны быть идентифицированы;*

*б) права доступа к объекту системы определяются на основании внешнего по отношению к системе правила.*

Большинство распространённых в настоящее время систем обеспечивает выполнение положений дискреционной политики безопасности в связи с простой реализацией соответствующих механизмов защиты. *Пример – матрица доступа*.

*Недостаток*этого типа политики безопасности – *статичность*модели: политика безопасности не учитывает динамику изменения состояния системы, не накладывает ограничения на её состояния.

**И при дискреционной политике *возникает вопрос*ОПРЕДЕЛЕНИЯ ПРАВИЛ РАСПРОСТРАНЕНИЯ ПРАВ ДОСТУПА *и АНАЛИЗА ИХ ВЛИЯНИЯ*НА БЕЗОПАСНОСТЬ системы.**

Перед МБО, который при санкционировании доступа к объекту руководствуется некоторым набором правил, стоит *алгоритмически неразрешимая задача*: проверить, приведут ли его действия к нарушению безопасности или нет.

Т. е., матрица доступов не является тем механизмом, который позволил бы реализовать ясную систему защиты информации в системе.

*Второй*тип политики безопасности – **это МАНДАТНАЯ (*полномочная)*политика безопасности**, которая составляет *мандатное управление доступом*. Англоязычная аббревиатура – *МАС*(*Mandatory access control*).

***Цель*мандатной политики безопасности** – устранить каналы *утечки*информация *сверху вниз*: информация не должна утекать от объектов с высоким уровнем доступа к объектам с низким уровнем доступа.

***Принципиальное отличие*систем *с мандатной*защитой от систем *с дискреционной*защитой:**

*если начальное состояние системы безопасно, и все переходы системы из состояния в состояние не нарушают ограничений, сформулированных политикой безопасности, то любое состояние системы безопасно*.

Для систем с мандатной политикой характерна более *высокая степень надёжности*, т. к. МБО такой системы ДОЛЖЕН ОТСЛЕЖИВАТЬ НЕ ТОЛЬКО ПРАВИЛА ОБРАЩЕНИЯ СУБЪЕКТОВ К ОБЪЕКТАМ, НО И СОСТОЯНИЯ САМОЙ АС (это модель системы под названием Белла Лапалуда).

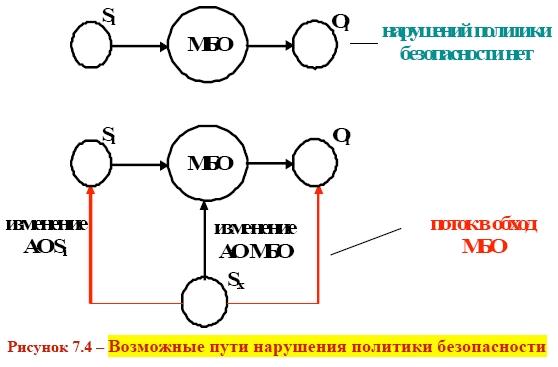
Т. е., каналы утечки в системах данного типа не заложены в ней непосредственно, а могут появиться только при практической реализации системы вследствие ошибок разработчика.

Но реализация систем с политикой безопасности данного типа сложна и требует значительных ресурсов.

## **7.3 Реализация политики безопасности**

Очевидно, что *при изменении функционально ассоциированных с монитором безопасности объектов*могут изменяться и свойства самого МБО, заключающиеся в фильтрации потоков.

Поэтому могут возникнуть потоки, принадлежащие некоторому подмножеству *N*, рисунок 7.4, где АО – ассоциированные объекты.



***Определение:***субъекты *Si и Sj*называются **невлияющими *друг на друга (или*корректными *относительно друг друга)****, если в любой момент времени отсутствует поток (изменяющий состояние объекта) между любыми объектами Oiи Oj, ассоциированными соответственно с субъектами Si и Sj*.

***Смысл понятия корректности*:** существующие в едином пространстве оперативной памяти программы не должны иметь функциональных возможностей изменения чужого вектора кода и состояния переменных.

*Субъекты Si и Sj называются****абсолютно корректными*(не влияющими друг на друга),** *если при прежних*(см. выше) *условиях*множества ассоциированных объектов *этих субъектов не имеют пересечения*. Абсолютная корректность *достижима в случае виртуального адресного пространства*.

72 Расшифровать шифртекст «ОВЯНВТИ\_ ЕМОНВ\_ЕРО\_КШЫВДАИЕЕЕСВ\_НЛААЕ\_АЮЕГК,ТТОТ\_СС\_ОКЯ, полученный методом одиночной перестановки по ключу (ключевое слово «ЛИНИЯ», размер таблицы 11 × 5).

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Л | И | Н | И | Я |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| О | Н | И | М | В | О | Ы | А | Е | В | А |
| В | В | \_ | О | Е | К | В | И | Е | Н | А |
| Я | Т | Е | Н | Р | Ш | Д | Е | С | Л | Е |
| А | Е | К | Т | О | С | О | Я |  |  |  |
| Ю | Г | , | Т | Т | С | К |  |  |  |  |

92 Зашифровать сообщение «КАРИНОЧКА», используя магический квадрат 3 ×3.