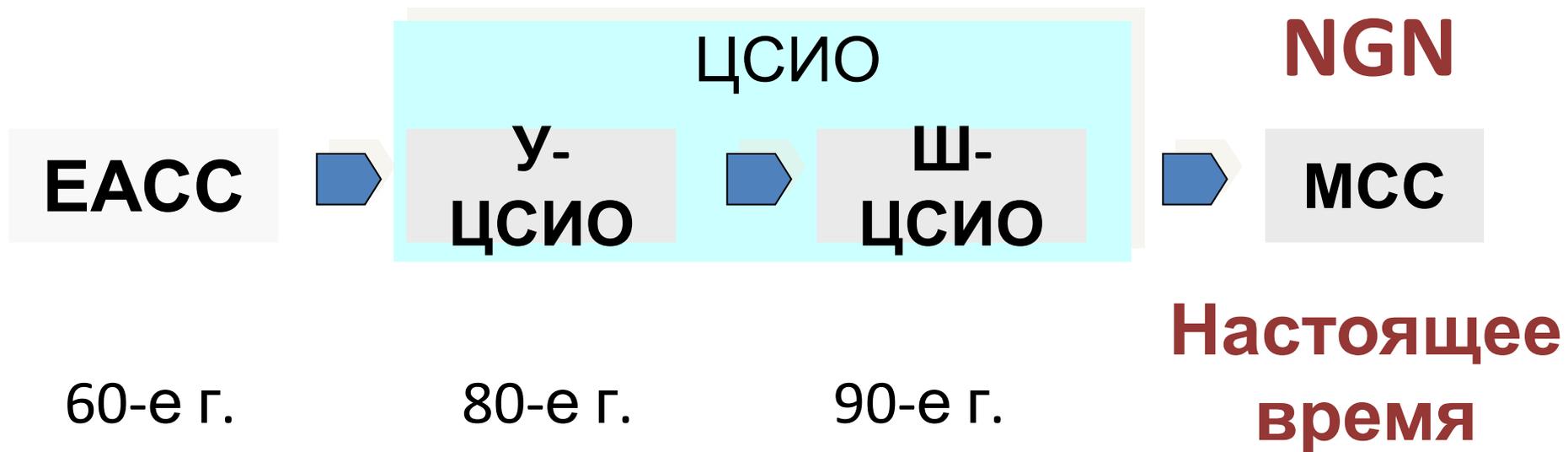
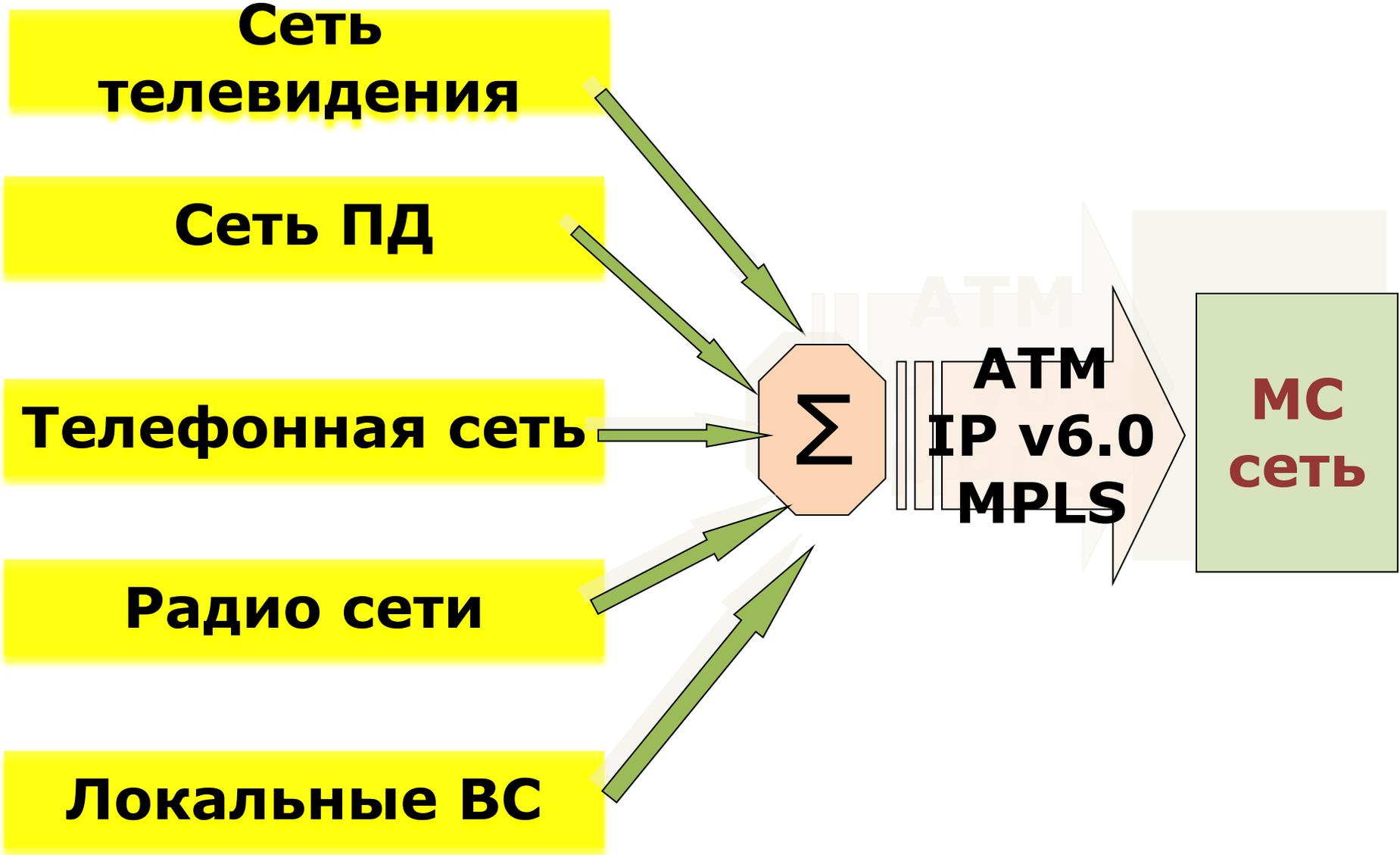


Введение в специальность «Информационная безопасность телекоммуникационны х систем»

Новиков С.Н. Кафедра
"БиУТ" ГОУ ВПО
"СибГУТИ"

Тенденции развития систем телекоммуникаций





МС сеть
СВЯЗИ

**Программа
«Электронная
Россия»
2000г.**

Видеоконференция

Электронная
коммерция

Дистанционное
обучение,
воспитание, тренаж,
реклама, развлечения

Видеотелефония

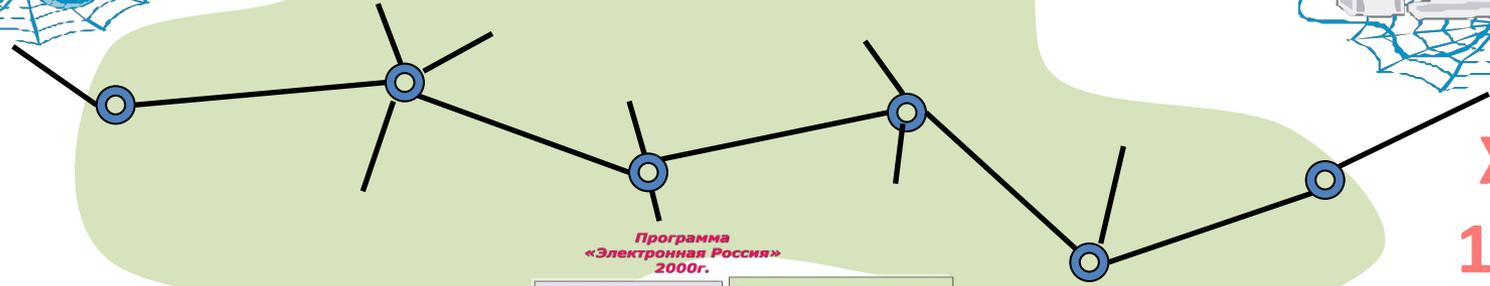
Телерадиовещани
е

Открытый доступ к институтам
управления государством

Поисковые службы (программных
продуктов,
документов, новости, видео, БД)



МС сеть связи



X.200
1984 г.

Программа
«Электронная Россия»
2000г.

- Видеоконференция
- Электронная коммерция
- Дистанционное обучение, воспитание, тренаж, реклама, развлечения
- Видеотелефония
- Телерадиовещание
- Открытый доступ к институтам управления государством
- Поисковые службы (программных продуктов, документов, новости, видео, БД)

У
р
о
в
н
и
в
о
с

Представления (6)

Прикладной (7)

Сеансовый (5)

Транспортный (4)

Сетевой (3)

Канальный (2)

Физический (1)

Особенности современных телекоммуникаций

- Интеграция услуг пользователю через единую точку доступа
- Гарантия качества предоставляемых услуг (ВВХ приложений)
- Мобильный доступ пользователя к услугам
- ИБ телекоммуникационных систем



а) Прерывание передачи информации



б) Перехват передаваемой информации

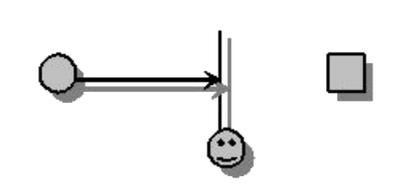


в) Модификация передаваемой информации



г) Фальсификация передаваемой информации

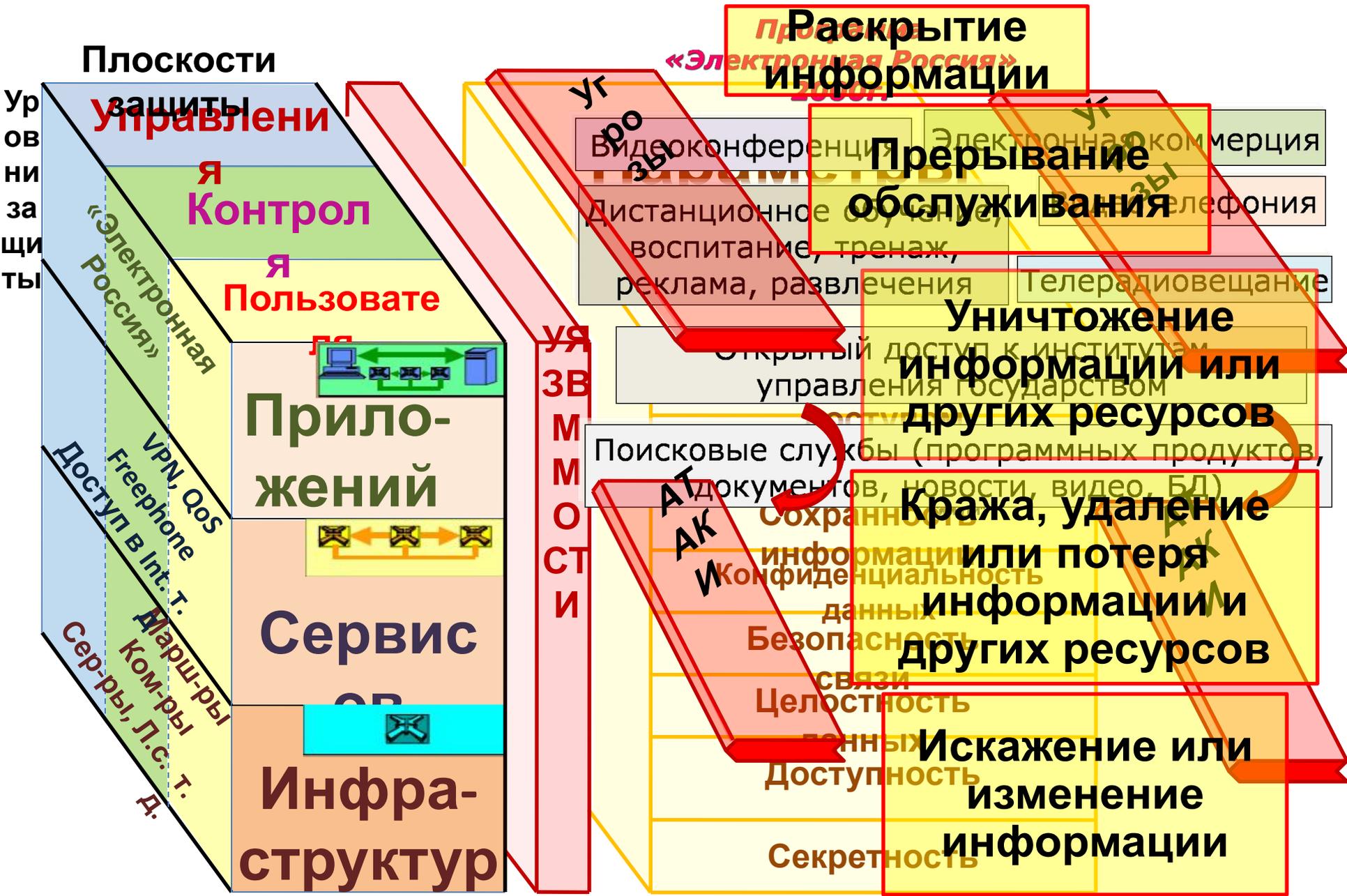
Таблица 4.1 - Классификация нарушений защиты информации

Виды нарушений	Активность нарушений	Графическое представление нарушений	Нарушение свойств информации
Перехват передаваемой информации	Пассивное		Конфиденциальность передаваемой информации
Прерывание передачи информации	Активные		Доступность информации
Модификация передаваемой информации			Конфиденциальность и целостность передаваемой информации
Фальсификация передаваемой информации			Аутентичность передаваемой информации

- **Управление доступом** – защищает от неправомерного использования сетевых ресурсов.
- **Аутентификация** – предназначено для удостоверения личностей поддерживающих связь объектов.
- **Сохранность информации** – гарантируется наличие данных, которые могут быть предоставлены третьей стороне и которые могут быть использованы как доказательство того, что некоторое

- **Конфиденциальность данных** – защищает данные от неправомерного раскрытия.
- **Безопасность связи** – гарантирует, что информация передается только между уполномоченными конечными точками.
- **Целостность данных** – гарантирует правильность и точность данных.

- **Доступность** – гарантирует отсутствие какого-либо ограничения на санкционированный доступ к элементам сети, хранимой информации, потокам данных, к услугам и приложениям из-за событий, влияющих на сеть.
- **Секретность** – обеспечивает защиту информации, которая могла бы быть получена, исходя из наблюдения сетевой деятельности.



Ы

Соотношение параметров защиты и угроз безопасности

(Какая защита необходима и от каких угроз?)

Параметры защиты	Угроза безопасности				
	Уничтожение информации	Искажение информации	Кража информации	Раскрытие информации	Прерывание обслуживания
Управление доступом	ДА	ДА	ДА	ДА	ДА
Аутентификация	ДА	ДА	ДА	ДА	ДА
Сохранность информации			ДА	ДА	
Конфиденциальность данных	ДА	ДА			ДА
Безопасность				ДА	

Применение архитектуры защиты к программам защиты



Архитектура защиты в табличной форме

	Уровень инфраструктуры	Уровень услуг	Уровень приложения
Плоскость управления	Модуль 1	Модуль 4	Модуль 7
Плоскость контроля	Модуль 2	Модуль 5	Модуль 8
Плоскость конечного пользователя	Модуль 3	Модуль 6	Модуль 9

Независимость модулей

Управление доступом	Безопасность связи
Аутентификация	Целостность данных
Сохранность информации	Доступность
Конфиденциальность данных	Секретность

Модуль 1

Управление доступом	Безопасность связи
Аутентификация	Целостность данных
Сохранность информации	Доступность
Конфиденциальность данных	Секретность



ы

Параметры защиты	Цель защиты (модуль 1)
Управление доступом	Гарантировать, что только уполномоченным <u>«пользователям»</u> разрешено выполнять административные действия или операции управления на СУ или ЛС.
Аутентификация	Проверять личность человека или устройства, выполняющего административные действия или операции управления на СУ или ЛС.
Сохранность информации	Формировать отчет, идентифицирующий человека или устройство, которые выполняют каждое административное действие или операцию управления на сетевом устройстве или ЛС, и действие, которое было выполнено.
Конфиденциальность данных	Защищать информацию о конфигурации сетевого устройства или ЛС от несанкционированного доступа и просмотра. Защищать информацию об аутентификации от несанкционированного доступа и просмотра.
Безопасность связи	При дистанционном управлении СУ или ЛС гарантировать, что управленческая информация передается только между станциями ДУ и устройствами или ЛС, управление которыми осуществляется.
Целостность данных	Защищать информацию о конфигурации СУ и ЛС от несанкционированной модификации, удаления, создания и дублирования. Эта защита применяется к информации о конфигурации, содержащейся СУ или ЛС, также к информации, которая передается транзитом или хранится автономно.
Доступность	Гарантировать, что уполномоченному <u>«пользователю»</u> не может быть отказано в способности управлять СУ или ЛС

Выводы

- **Максимальная защищенность ТКС обеспечивается полной реализацией АЗ.**
- **Каждый уровень АЗ имеет различные точки уязвимости защиты.**
- **При проектировании и эксплуатации ТКС необходимо учитывать, чтобы события в одной плоскости и в одном уровне АЗ были полностью изолированы от других плоскостей и уровней (независимость модулей).**

**Благодарю за
внимание!**