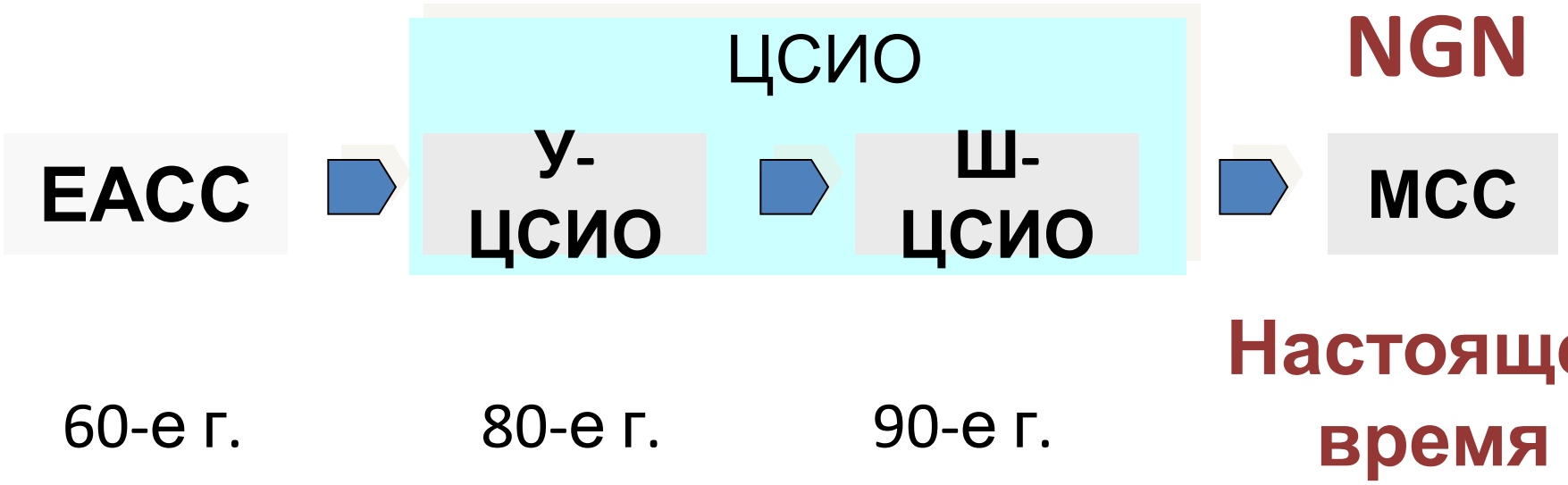
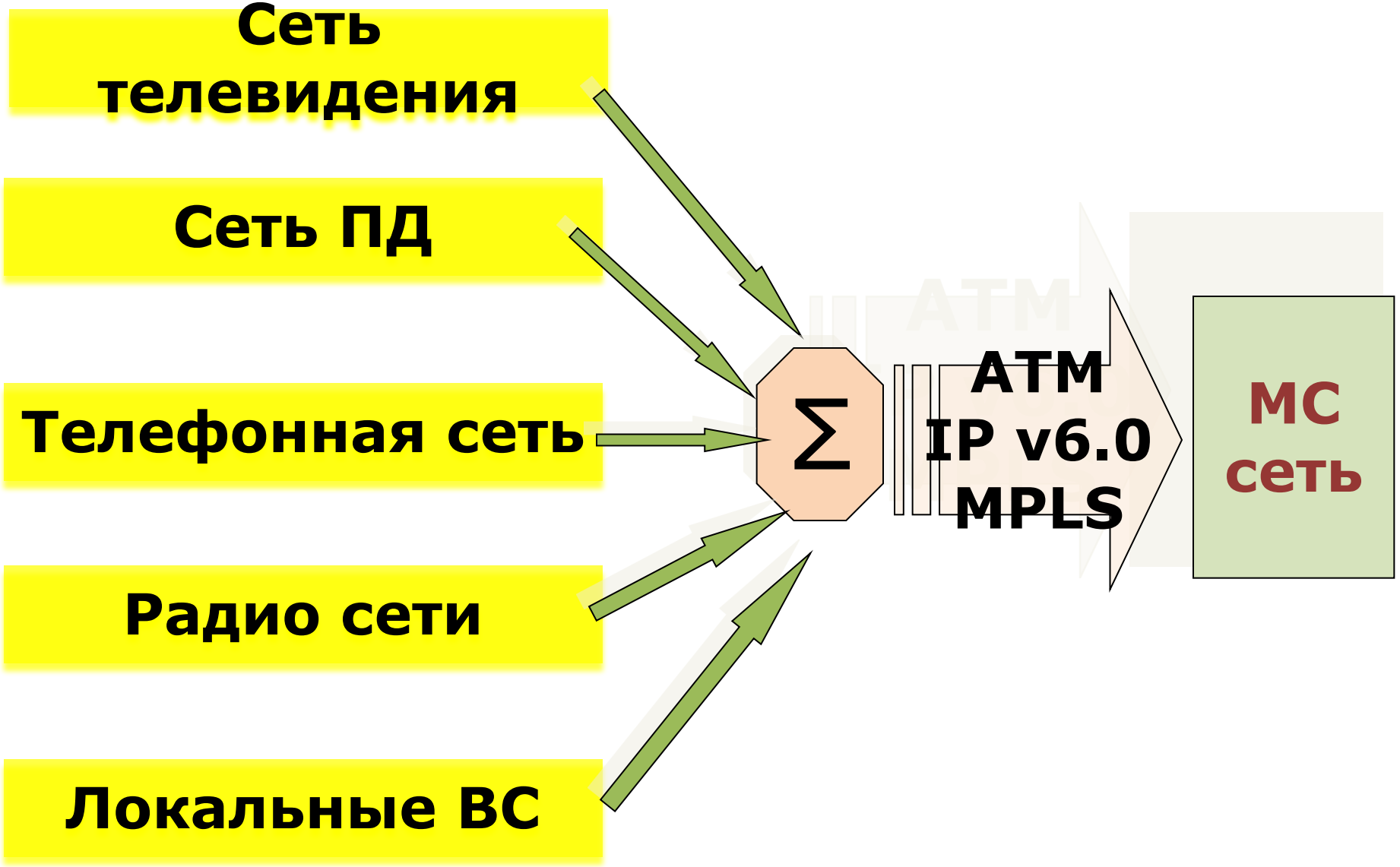
Введение в специальность «Информационная безопасность телекоммуникационных систем»

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

Тенденции развития систем телекоммуникаций




Сеть телевидения
Сеть ПД
Телефонная сеть
Радио сети
Локальные ВС
Σ
ATM
IP v6.0
MPLS
МС сеть

МС сеть связи

Программа «Электронная Россия» 2000г.

Электронная коммерция

Видеоконференция

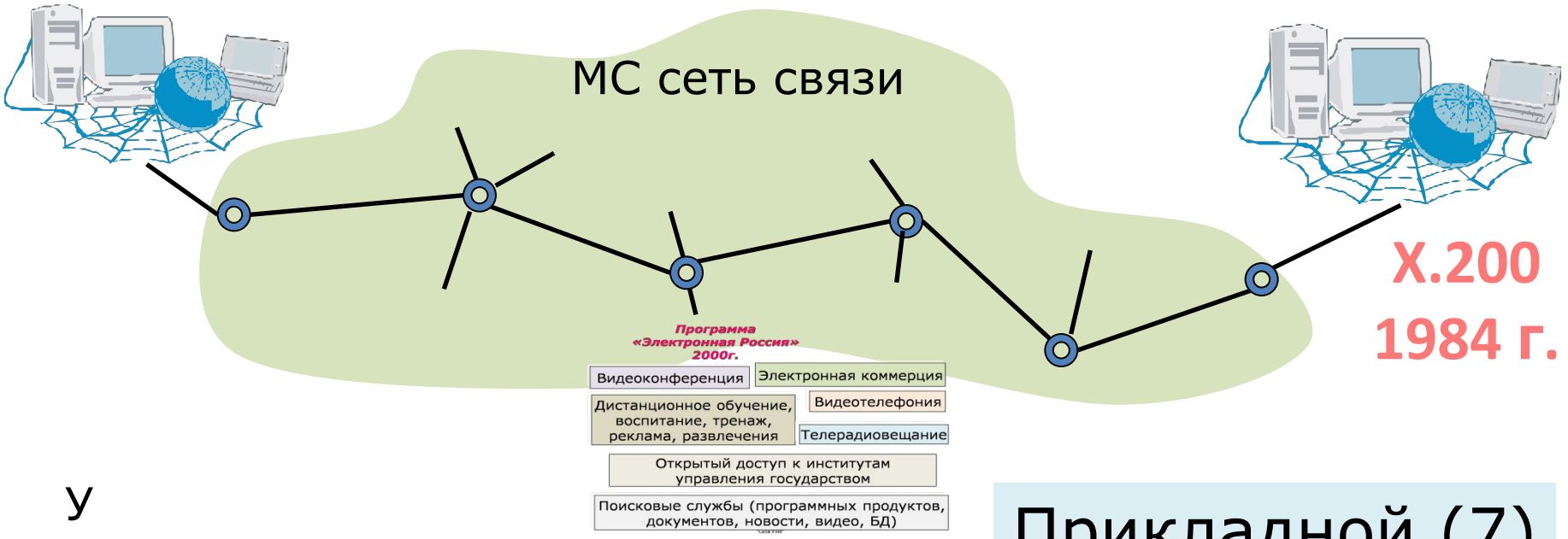
Дистанционное обучение, воспитание, тренаж, реклама, развлечения

Видеотелефония

Телерадиовещание

Открытый доступ к институтам управления государством

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



X.200
1984 г.

Уровни ВОС

Прикладной (7)

Представления (6)

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

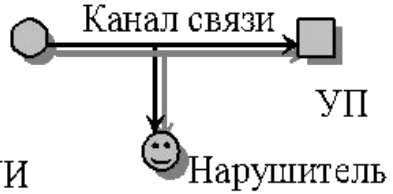
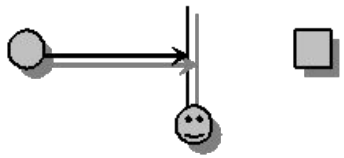
б) Перехват передаваемой информации

в) Модификация передаваемой информации

г) Фальсификация передаваемой информации

Рисунок 4.3 — Виды нарушений передачи 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 неправомочного 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 использоваться как доказательства того, что некоторое**

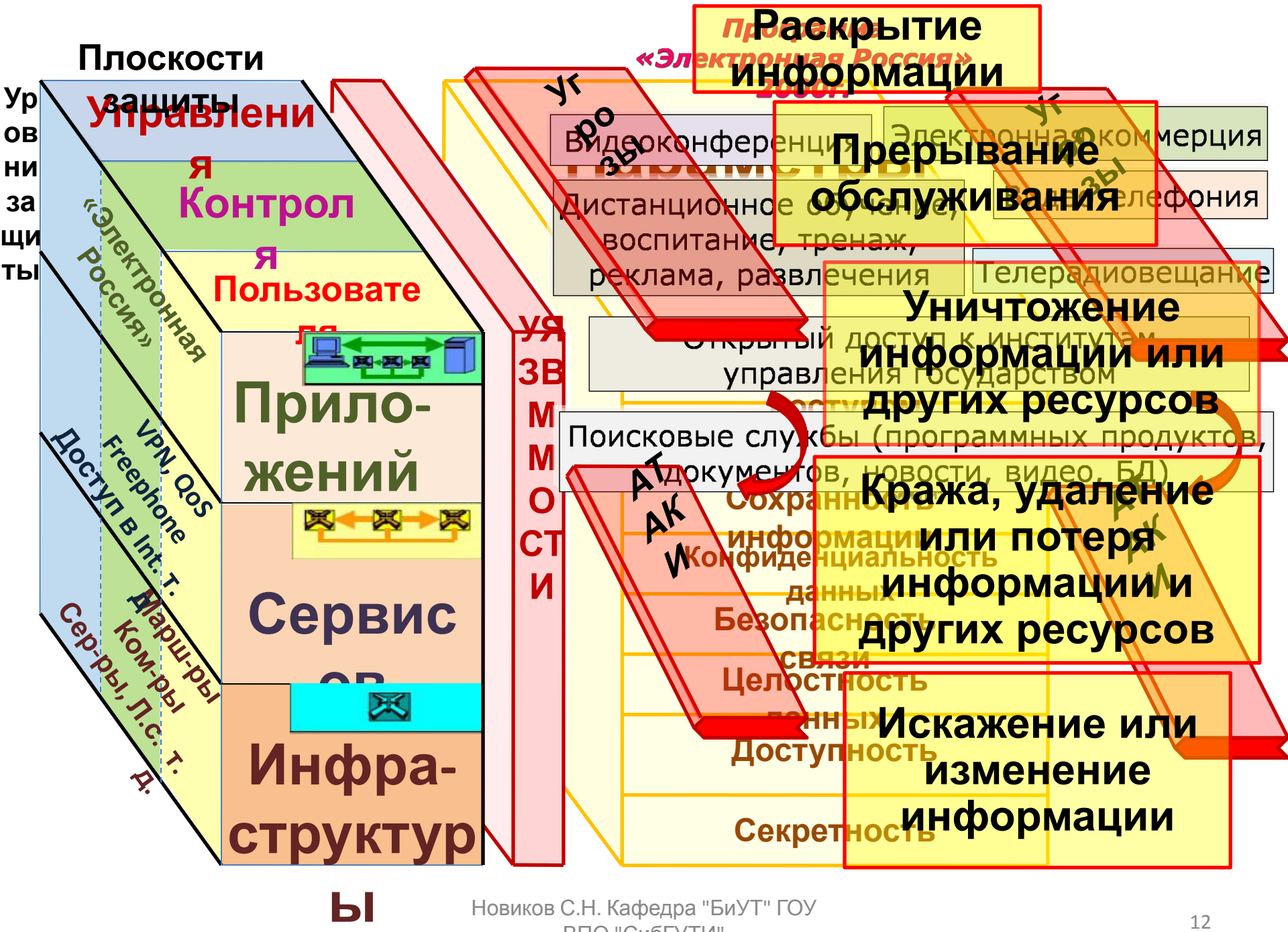
- **Конфиденциальность данных** – защищает данные от неправомочного раскрытия.

- **Безопасность связи** – гарантирует, что информация передается только между уполномоченными оконечными 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.**


Плоскости защиты
Уровни защиты
Управления
Контроля
Пользователя
Прило-жений
Сервисов
Инфра-структуры
«Электронная Россия»
VPN, QoS
Freephone
Доступ в Int. т.
Марш-ры
Ком-ры
Сер-ры, Л.с. т. д.
Уязвимости
Угрозы
Атаки
Программа «Электронная Россия» 2002г.
Видеоконференция
Электронная коммерция
Дистанционное обучение, воспитание, тренаж, реклама, развлечения
Телефония
Телерадиовещание
Открытый доступ к институтам управления государством
Поисковые службы (программных продуктов, документов, новости, видео, БД)
Сохранность информации
Конфиденциальность данных
Безопасность связи
Целостность данных
Доступность
Секретность
Раскрытие информации
Прерывание обслуживания
Уничтожение информации или других ресурсов
Кража, удаление или потеря информации и других ресурсов
Искажение или изменение информации

Соотношение параметров защиты и угроз безопасности

(Какая защита необходима и от каких угроз?)

Пара-метры защиты	Угроза безопасности				
	Уничтожение информации	Искажение информации	Кража информации	Раскрытие информации	Прерывание обсл-вания
Управление доступом	ДА	ДА	ДА	ДА	
Аутенти-фикация	ДА	ДА	ДА	ДА	ДА
Сохранность информации			ДА ДА	ДА ДА	
Конфиден-циальность данных	ДА ДА	ДА			ДА
Безопас-ность				ДА	

Применение архитектуры защиты к программам защиты

Архитектура защиты в табличной форме

	Уровень инфраструктуры	Уровень услуг	Уровень приложений
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

Параметры защиты	Цель защиты (модуль 1)
Управление доступом	Гарантировать, что только уполномоченным ***«пользователям»*** разрешено выполнять административные действия или операции управления на СУ или ЛС.
Аутенти-фикация	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.
Конфиден-циальность 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.
Доступност	Гарантировать, что уполномоченному ***«пользователю»*** 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!