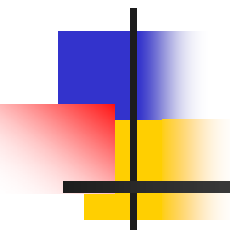


ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ДОВЕРИЕ В ТАРИФИКАЦИОННОЙ ПОЛИТИКЕ И МЕЖСЕТЕВОМ ВЗАИМОДЕЙСТВИИ ОПЕРАТОРОВ ТЕЛЕКОМУНИКАЦИЙ



Владимир Кононович – канд. техн. наук,

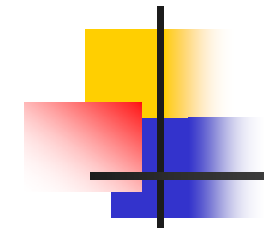
член-корреспондент

Академии связи Украины – відділення

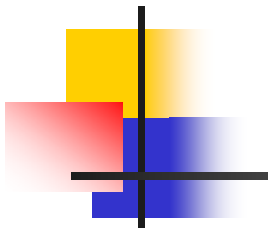
Міжнародної Академії інформатизації,

асоційованого члена ООН

Содержание доклада:



- 1 Система информационной безопасности телекоммуникаций (по материалам ITU-T, ISO, IEC)
- 2 Информационная безопасность системы контроля и менеджмента телекоммуникационных услуг и тарификации
- 3 Международная сертификация системы информационной безопасности как мера доверия при взаимодействии операторов
- 4 Договор о взаимной защите информации при взаимодействии операторов телекоммуникаций



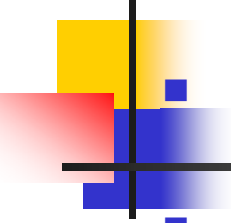
Целью работы есть анализ обеспечения информационной безопасности телекоммуникаций при взаимодействиях операторов телекоммуникаций с позиций укрепления доверия и повышения эффективности предоставления телекоммуникационных услуг

Материалами для доклада послужили работы, проведенные ОНАЗ и Одесским РЦ ТЗИ в сфере создания комплексных систем защиты информации в телекоммуникационных сетях общего пользования и в корпоративной сети передачи данных, которые финансировались ВАТ «Укртелеком».



ITU-T (CCITT) Recommendation

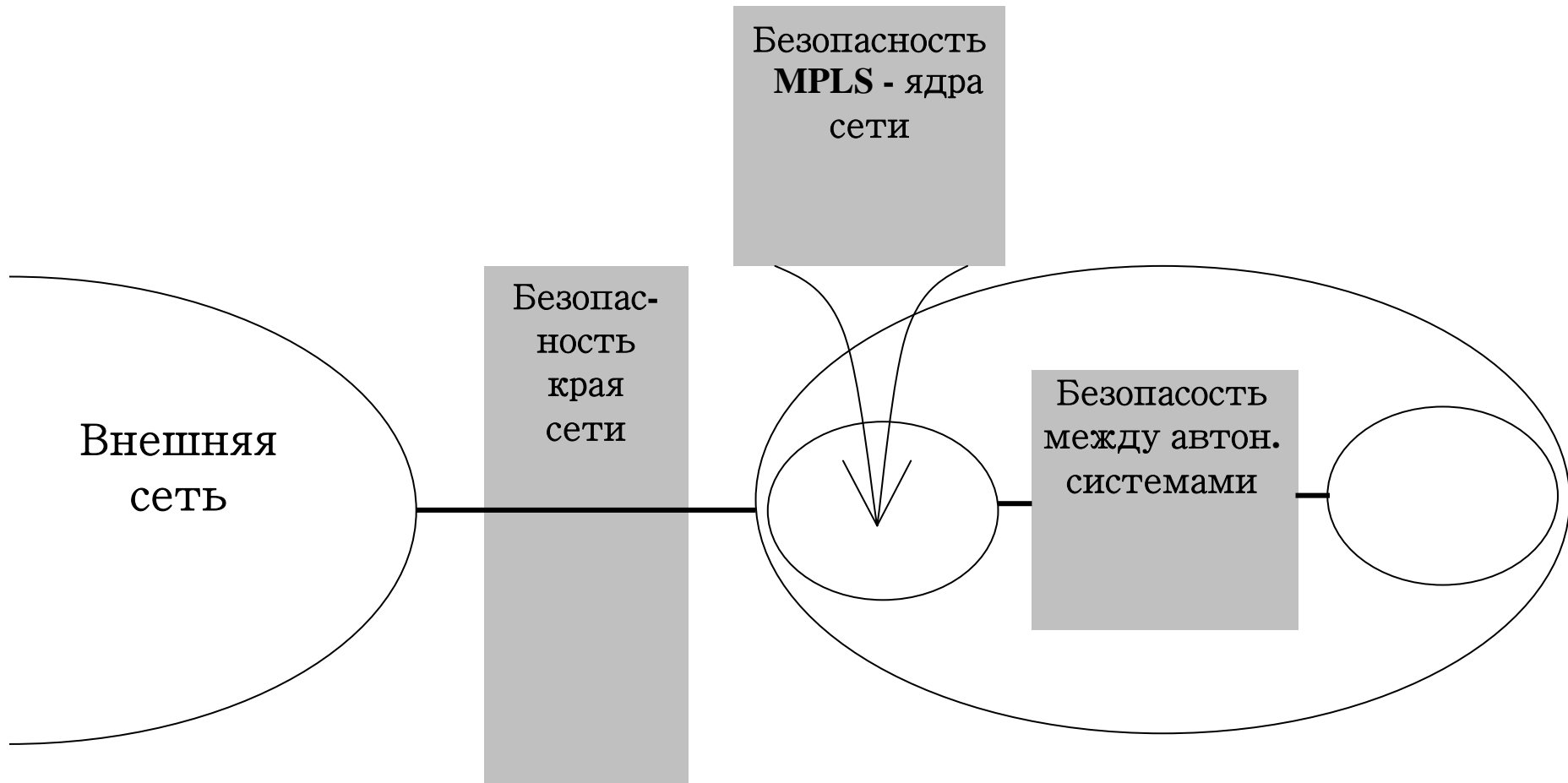
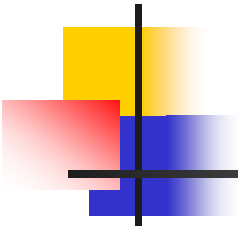
- **X.800.** Архитектура безопасности ВОС
- **X.805.** Security architecture for end-to-end communications
- **E.408.** Требования к безопасности сетей электросвязи
- **E.409.** Организация реагирования на инциденты и обработка инцидентов безопасности
- **Y.1711.** Механизм эксплуатации и техобслуживания для сетей MPLS
- **Y.1720.** Protection switching for MPLS networks
- **H.235** — Security and Encryption for H.323 multimedia terminals

- 
- ДСТУ ISO 15408-1: 2005. Вступ і загальна модель.
 - ДСТУ ISO 15408-2: 2005. Функціональні вимоги безпеки.
 - ДСТУ ISO 15408-3: 2005. Вимоги до забезпечення захисту.
 - ДСТУ ISO/IEC 17799 Практичні рекомендації з управління ІБ
 - ДСТУ ISO/IEC TR 13335-1 Концепції і моделі безпеки..
 - ДСТУ ISO/IEC TR 13335-2: Керування та планування безпеки.
 - ДСТУ ISO/IEC TR 13335-3 Методи керування захистом.
 - ДСТУ ISO/IEC TR 13335-4 Вибирання засобів захисту.
 - ДСТУ ISO/IEC TR 13335-5 Настанова з управління мережною безпекою.
 - ISO/IEC 27001. Information security management systems. Requirements.
 - ISO/IEC TR 18044:2004. Information security incident management.

Стандарти о реагировании на инциденты информационной безопасности



Структура безопасности сети MPLS





С точки зрения безопасности технология MPLS делится на:

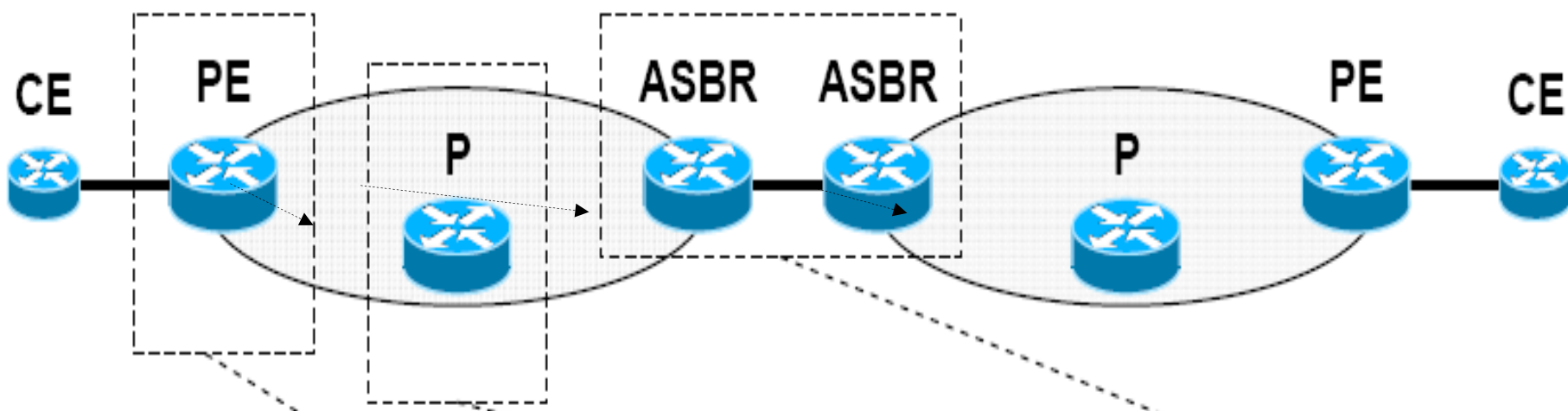
- инфраструктуру ядра MPLS, которая имеет границу, образованную пограничными элементами.
- внешние, относительно ядра MPLS, сети
- соединения внешних сетей с пограничными элементами ядра сети MPLS



Группы требований к безопасности элементов сети MPLS

- Безопасность края сети MPLS, в точке демаркации между национальным доменом и внешней сетью
- Безопасность ядра сети MPLS для соединения из конца в конец
- Безопасность inter-AS/SP MPLS сети между доменами автономных систем

Фрагмент сети из взаимодействующих доменов двух стран, построенной по технологии MPLS



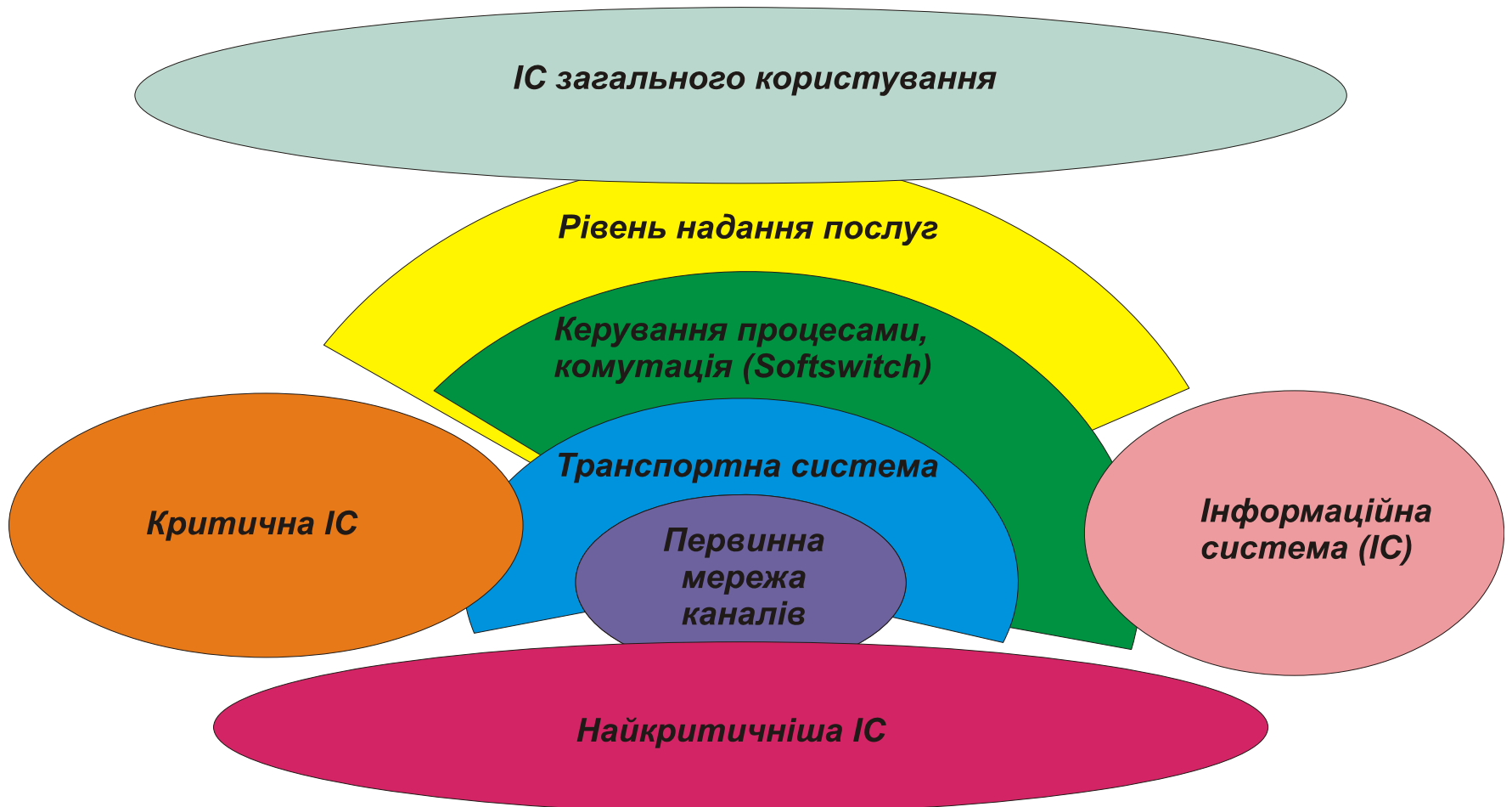
CE – Customer Edge – маршрутизатор конечного пользователя

Пограничные услуги MPLS (маршрутизатор PE)

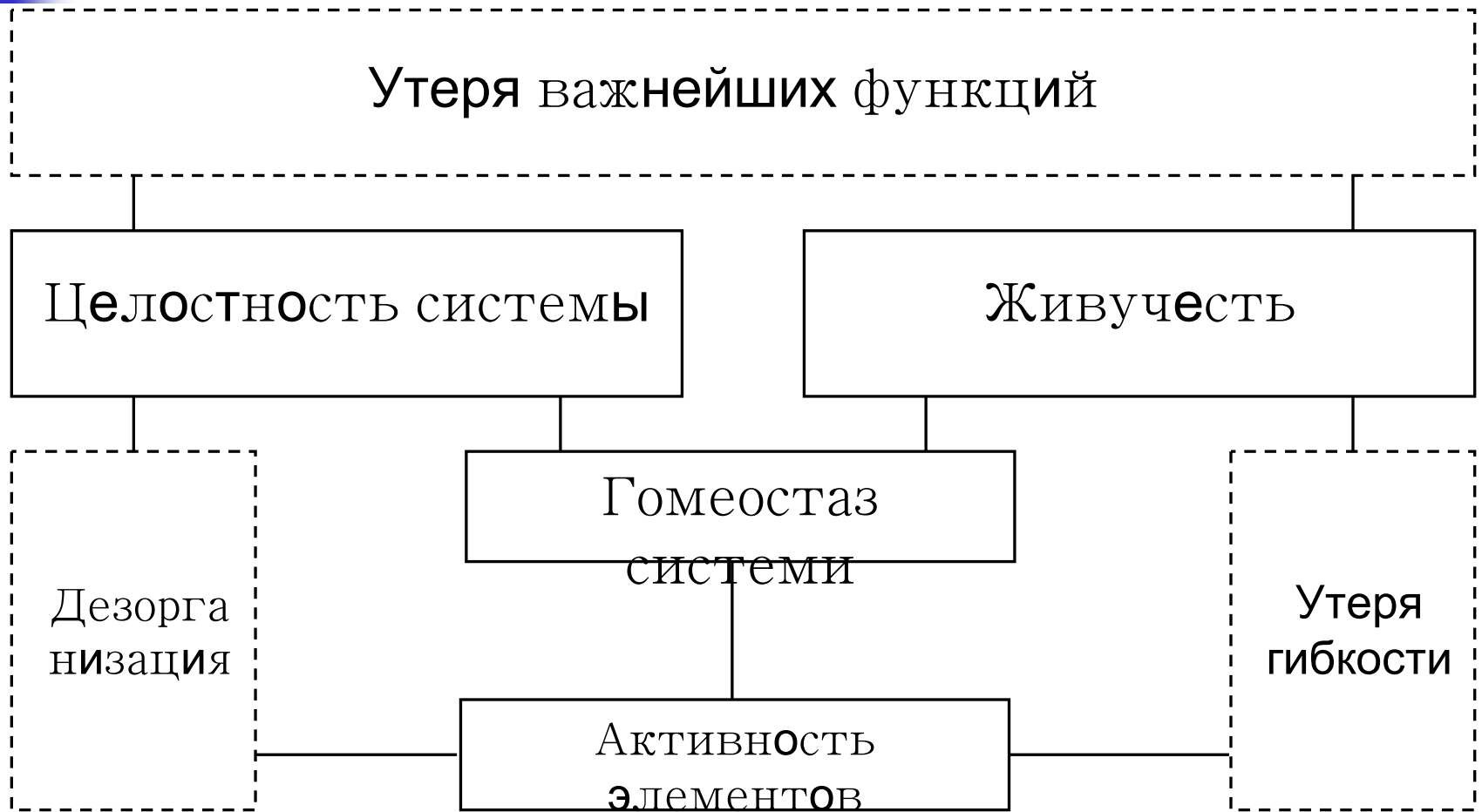
Ядро MPLS (внутренний маршрутизатор P)

Пограничный inter-AS MPLS.
Соглашение SLA.
Условия TCA.
Соглашение о безопасности

Распределение ответственности за информационную безопасность



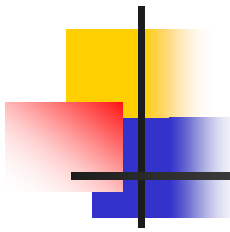
Живучесть телекоммуникационных систем





Телекоммуникации – наиболее критичный ресурс

- Критические технологии - это технологии, определенные в установленном законодательством порядке как такие, что обеспечивают определяющий вклад в достижение конкретных целей в сфере обеспечения национальной безопасности, экономического и социального развития государства, в решение важнейших проблем реализации приоритетных направлений развития науки и техники



*Наиболее важной является проблема
управления инцидентами безопасности
в телекоммуникационной сети*

- Ни какая система обеспечения информационной безопасности (СОИБ) принципиально не может гарантировать стопроцентной защиты.
- Даже после внедрения СОИБ все равно остаются риски, которые делают возможным возникновение инцидентов безопасности телекоммуникационной сети

СЕРИЯ Е: ОБЩАЯ ЭКСПЛУАТАЦИЯ СЕТИ,
ТЕЛЕФОННАЯ СЛУЖБА, ФУНКЦИОНИРОВАНИЕ
СЛУЖБ И ЧЕЛОВЕЧЕСКИЕ ФАКТОРЫ

Управление сетью

- **Рекомендация МСЭ-Т Е.408**
Требования к безопасности сетей
электросвязи

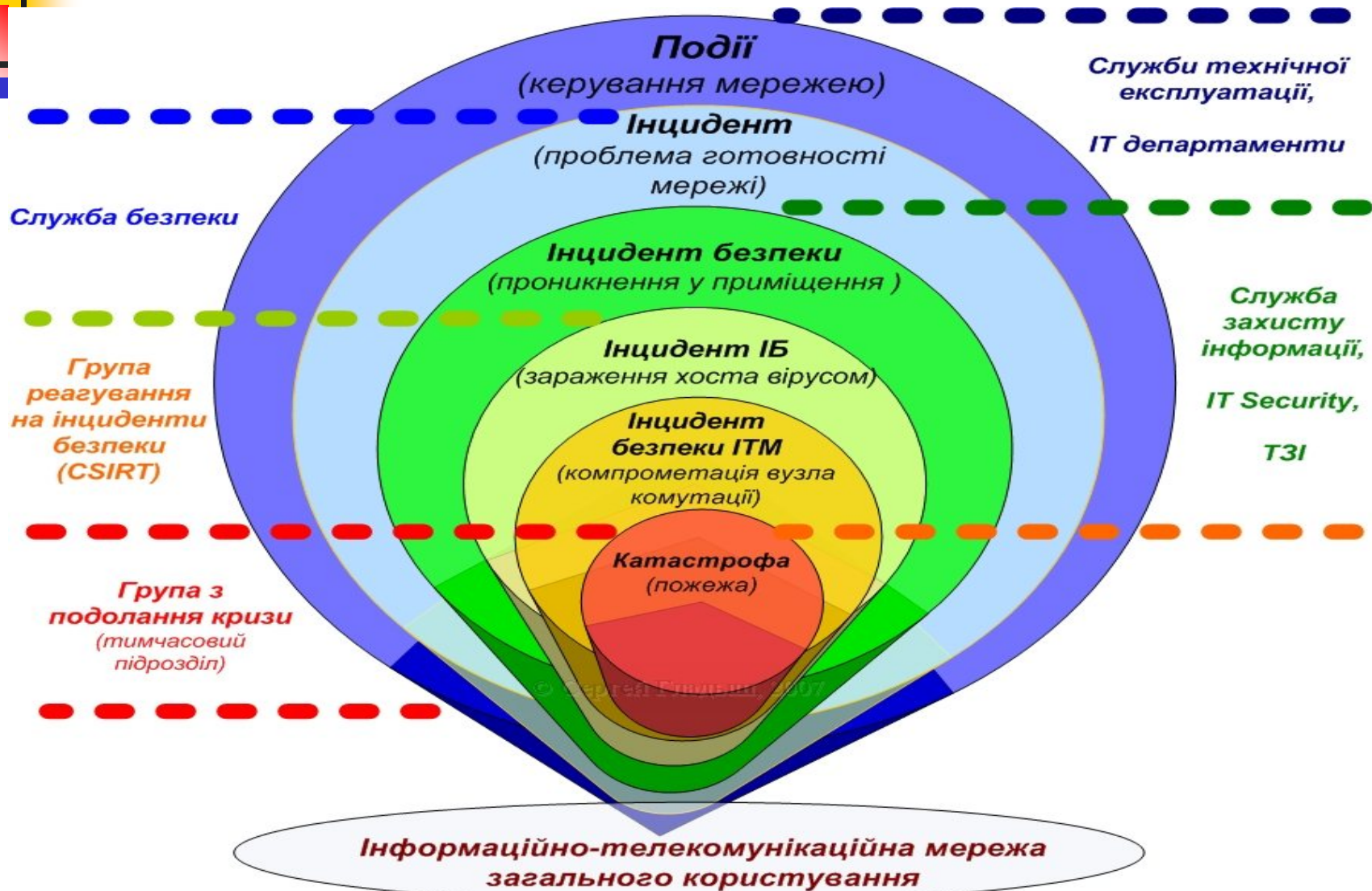
- **Рекомендация МСЭ-Т Е.409**

Организация по реагированию на
инциденты и обработка инцидентов
безопасности: Руководство
для организаций электросвязи

Распределение заданий информационной безопасности



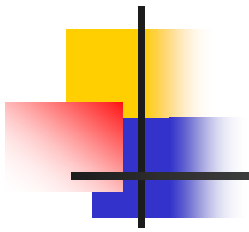
Иерархия инцидентов и распределение ответственности



Структура обробки інцидента безпеки



Автоматизированный почасовой учет разговоров



База данных системы содержит информацию относительно:

- количества и суммарной длительности, времени и номеру набора переговоров;
- неисправности разговорного тракта АТС (абонентных и шнуровых комплектов) и таксофонов;
- данных нагрузки абонентских комплектов;
- присвоенных категорий абонентов;
- технического состояния самой системы.



Защита информации требует расходов дополнительных ресурсов.

- Практика показывает, что для получения приемлемого уровня защищенности информации целесообразно тратить не более 20% от общих расходов на информационную систему

Договор о взаимной защите информации

- - *преамбула*
- - *цель и предмет договора*
- - *сфера использования договора- определение терминов*
- - *уполномоченные органы в сфере информационной безопасности*
- - *контракты (соглашения)*
- - *непосредственная связь договора с другими контрактами*
- - *степень защищенности*
- - *использование передаваемой информации- передача информации и материалов;*
- - *хранение информации и материалов- ознакомление с информацией и материалами*
- - *нарушения правил безопасности*
- - *визиты*
- - *общие требования, (при необходимости, например, консультаций)*
- - *затраты на проведение защиты*
- - *решение спорных вопросов*
- - *изменения и дополнения*
- - *срок действия и прекращения договора, утверждения, подписи*



Дякую за увагу!

Володимир Кононович

Контакти через ОНАС

Тел. (8-048) 761-01-01

E-mail: kononovich@mail.ru