ИНФОРМТЕХНИКА
informtekhnika

«Проблемы информационной безопасности и импортозамещения оборудования систем связи АЭС»

к.т.н.Кривошапко В.М.
kvm@infotek.ru
+7(495)6466731 доб.3044
+7(915)3512166

Конференция «Атомстройстандарт-2015»

Оглавление

1. Виды и подсистемы внутриобъектной связи АЭС

Контуры управления, подсистемы и виды связи АЭС		Проводная					Беспроводная	
		Аудио			Видео		Микросотовая	Сотовая
		Двусторонняя		Односторонняя громкая	Двусторонняя	Односторонняя		
		Тихая	Громкая					
Задачи внутриобъектного управления (связи)	1.Подсистема Общестанционной Связи (ОбС)	1.Общестанционная телефонная связь 2.ОбТС 3.CYA	1.Связь совещаний. 2.СС	1.Радиотрансляция 2.РТ 3.CYN	1.Видеоконференцсвязь 2.ВКС	1. Кабельное телевидение 2.КТВ	1.Общестанционнная радиосвязь 2. ОБС РС (GSM,DECT) 3.CYY	GSM
	2.Подсистема Оперативно-технологической Связи (ОС)	1. Оперативная телефонная связь 2.ОТС 3.CYB	1.Двусторонняя громкоговорящая связь 2.ДГС 3.CYB	1.Командно-поисковая связь 2.КПС 3.CYC		1.Промтелевидение 2. ПТВ 3. CYP		1.Оперативная радиосвязь 2. ОС РС (TETRA, GSM-R,…). 3. CYS
	3.Подсистема Оперативной Связи ПротивоАврийного Управления (ОСПАУ)	1.Оперативная телефонная связь ПАУ 2. ОТСПАУ 3. CYB	-	1. Оповещение 2. ОПОВ 3. CYC	1.Телемост ПАУ	1.Телеоповещение		1.Радиосвязь ПАУ 2. ОС РСПАУ 3.CYS
Задачи управления спецбезопасности	4.Подсистема Оперативнай Связи Физической Защиты (ОСФЗ)	Прямая телефонная CZG		Громкая связь CZC		Охранное телевидение CZE		Оперативная радиосвязь CZS

Референс “Информтехники”: АЭС Бушер, АЭС Куданкулам, Балаковская АЭС, ЛАЭС-2, Красноярский ГХК

Актуальность проблемы импортозамещения- конкурентная среда

Код KKS, наименование вида связи	Объем рынка, млрд.руб. в год.	% импорта	Иностранное оборудование	Отечественное оборудование
CYA, CYB, CZG - телефонная и двустроняя громкая связь	0,5-1	60%	Avaya (США), Siemens (Германия), Coral (Израиль), Huaiwei (КНР), Panasonic (Япония), Cisco (США)	1. МиниКом DX-500 (MX-1000). 2,3.Протон, Квант
CYC, CYN, CZS- оповещение и ко-мандный поиск	0,3-0,6	50%	"Industronics" (Германия), Neumann (Германия), Coral (Израиль), ProCom (Германия)	1.МиниКом DX-500 2-4.Элес, Арман, Эскорт
CYY- микросотовая связь DECT	0,2-0,3	40%	Ascom (Швейцария), Unify (бывший Siemens) (Германия), Aastra (Канада), RTX (Дания)	1.МиниКом DECT 2.Гудвин
CYS, CZS- транкинговая радиосвязь TETRA и DMR	0,2-0,4	90%	Motorola (США), Selex (Италия), Hytera (КНР), Damn (Дания)	1.МиниКом TETRA 2,3.Калугаприбор, Ижевский радиозавод
Всего	1,2-2,3	>60%		

1. Импортное оборудование задало планку высокого качества, в “тучные” годы сложилось доминирование импортного оборудования (особенно- РС, ССФЗ).
2. За последние 10-15 лет во всех нишах появилось конкурентное отечественное оборудование и происходит постепенное импортозамещение. Целенаправленных программ импортозамещения в отрасли нет.

2.Модель инфобезопасности: объект, уязвимости и угрозы

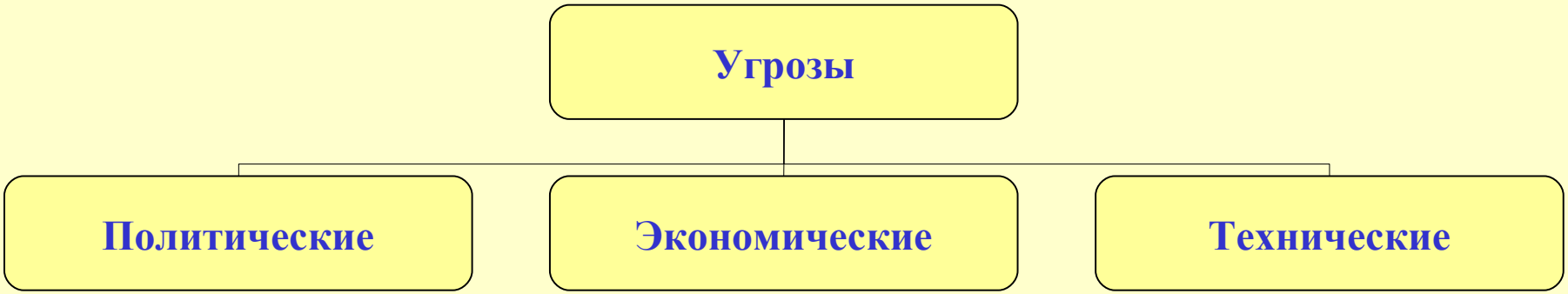
1.Система связи: АТС, СУ, ТО, АО, РО

2. Модель “уязвимости”	
Система связи (КЗ-НКЗ)	**Информация (речевая):**
1.СУ 2.АТС, ТО, (РО) 3. АО	**1.Для оповещения: -доступность; -целостность. 2.Для переговоров: -конфиденциальность**

3. Модель “угроз”		
Антропо (ЧФ)	**Техно**	**Природа**
-НСД (НПД) -НДВ -ЭМИ (ПМИН) -ШТ (шифротехника); -политико-экономические	**Аварии**	**Природные катаклизмы**

Модель уязвимости и средств обеспечения ИБ оборудования связи

Структура угроз мпортозависимости оборудования систем связи АЭС



Эмбарго полное: Роснефть, МО (Мистрали)	Девальвация рубля	Потеря технической независимости
Эмбарго частичное: Газпром, ВПК, Техснабэкспорт (Росатом)	Бюджетный кризис	Уязвимость инфобезопасности оборудования связи (НСД, НДВ, ПМИН, ШТ)
Угроза эмбарго: весь high tech (прекращение техподдержки и поставки ИП)	Платежные системы (SWIFT, etc)	Защита информации (Секретно, Конфиденциально, Общедоступно)

1. Бесконтрольное применение импортного оборудования приводит к непоправимым рискам.
2. Девальвация рубля является главной движущей силой импортозамещения.
3. В ИТТ/ТЗ на оборудование связи АЭС практически игнорируются политические и технические риски применения импортного оборудования.

Основные угрозы для оборудования систем связи (СС) АЭС и меры их компенсации

N	Приоритеты угроз	Критические системы связи	Достаточная компенсирующая мера	Необходимая компенсирующая мера	Предложения в НТД (ИТТ/ТЗ)
1	Прекращение техподдержки и поставки ЗИП для оборудования длительного применения	1.Все системы (кроме общестанционного управления СУА)	Импортозамещение	1.Резервирование подсистем связи. 2.Исключение применения нестандартного оборудования. Наличие более 2-х изготовителей.	1.Гарантия (декларация) изготовителя оборудования о предоставлении техподдержки и поставки ЗИП на период срока службы (10-20 лет).
2	Вывод оборудования из работоспособного состояния внешним воздействием в особый период	1.Физзиащита (CZG,CZS) 2.Противоаварийное управление (CYB, CYS)	Спецустойчивость (спецпроверка): Сертификат ФСБ и/или ФСТЭК об отсутствии в системе управления факторов НСД и НДВ	1.Предоставление исходных кодов ПО. 2.Применение доверенного оборудования.	1.Декларация изготовителя оборудования об отсутствии факторов НСД и НДВ в ПО.
3	Незащищенность информации (ДСП или С) в оборудовании связи	1.Физзиащита (CZG,CZS) 2.Противоаварийное управление (CYS)	Сертификат ФСБ о применении для работы с закрытой информации	1.Предоставление исходных кодов ПО. 2.Применение доверенного оборудования.	1. Обязательная проработка раздела информационная безопасность в ИТТ/ТЗ.

Для всех случаев необходимое условие- развитие конкурентной отечественной промышленности.

3.Система требований к инфобезопасности оборудования СС АЭС

Основные контуры управления (системы связи) АЭС		Мягкие (нетехнические) факторы		Жесткие (технические) факторы			
		Гарантия обеспечения техподдержки и поставки ЗИП на срок службы	Гарантии предоставления исходных кодов ПО	НСД- Сертификат ФСТЭК на класс защита от несанкционированного доступа	НДВ (и НСД) Сертификат ФСБ на отсутствие недекларированных возможностей	ПЭМИН- Сертификат Гос-техкомиссии на минимальность побочных электромагнитных излучений и наводок	ШТ- шифротехника сертификат ФСБ
Оперативно-технологический и ПА- открыто	CYB (ОТС+ДГС) МиниКом DX-500	+	+	?	-	-	-
	CYS (Оперативная РС) МиниКом TETRA)	+	+	?			?-E2E в радиоканале
Физзащита-частично ДСП	CZG (Прямая телефонная связь) МиниКом DX-500(А2)	+	+	Сертификат А2 (ФСБ) для подсистемы (ДСП)		Не требуется	
	CZS (Радиосвязь DMR и TETRA)	+	+	Сертификат А2 (ФСБ) для подсистемы (ДСП)		Возможно требуется	
Спец--связь-Секретно	Спецтелефонная связь (МиниКом DX-500С)	+	+	Сертификат ФСБ			
	Спецрадиосвязь (МиниКом TETRA)	+	+	Сертификат ФСБ			

Система требований в отрасли плохо проработана- не учитывает риски эмбарго

“Связь” vs “АСУТП”

Уровни формирования свойств объекта
Система
Оборудование
Модуль
БИС, компонент

HW	Системное
SW	Прикладное

1. Методология обеспечения инфобезопасности оборудования связи и АСУТП аналогична.
2. Ethernet-- единая технология транспорта для связи и АСУТП (АСУП).

“Инфобезопасность” vs ”Импортозамещение”

Инфобезопасность (Кибербезопасность)	
Встроенная (управляемая) (ТЗ, СТП, …)	Невстроенная (неуправляемая) (? фактическая)
Отечественное оборудование	Импортное оборудование
Импортозамещение (Импортозависимость)	

1.Отечественное происхождение оборудование- необходимое условие обеспечение инфобезопасности.

2.Полномочия присвоения статуса телекоммуникационного оборудования отечественного происхождения имеет только спецкомиссия Минпромторга РФ.

“Критичность-Затраты (%)”для задач импортозамещения

Критичность	Связь (15%)	АСУТП (50%)	АСУП (40%)
1.Контур физзащиты (спецустойчивость-инфобезопасность)	10%	?	?
2.Контур противоаварийного управления (спецустойчивость-инфобезопасность)	5%	?	?
3.Контур оперативно-технологического управления (спеустойчивость)	70%	?	
4.Контур администатривно-хозяйственного управления (цена)	15%		

1.Наиболее критичными для импортозамещения являются системы связи ФЗ и противоаварийного управления, далее соответствующие системы АСУТП.

2. Сейчас в отрасли актуальной стала задача обеспечения кибербезопасности АСУТП.

Механизмы в Росатоме-Росэнергоатоме

1. Технические:

-нет во многих ИТТ/ТЗ требований в части инфобезопасности (отраслевая TETRA, PC, СПТС,..);

+ВВЭР ТОИ; ТЗ Кибербезопасность.

2. Экономические:

-нет в ЕОСЗ преференций отечественному оборудованию (срок службы 10 лет- долговременный ЗИП и техподдержка)

+программа импортозамещения для строительного (нетехнологического) оборудования (СРО “АТОМСТРОЙ”, etc).

3. Организационные:

-Разрешение на применение импортных комплектующих в соответствии РД 036)- неадекватны и имеют обратное действие:

+нужны от Ростехнадзора и РЭА перечни запрещенных компонентов (СБИС с закладками, ПО с недекларируемы-ми возможностями, etc) и перечни запрещенных производителей-поставщиков.

Подход ГК “Информтехника”

1. Иерархический подход к обеспечению инфобезопасности.
2. Плавный уход из рисковых стран (ориентация на ЮВА,.., Intel CISC->PRC RISC).
3. Собственные разработки HW и SW.
4. Использование Open Source SW (Linux и др.), открытых HW архитектур (ADTCI, etc).
5. Собственное производство с элементами контрактного поверхностного монтажа (SMT).
6. Использование FPGA для проектирования- производства защищенных маршрутизаторов.
7. OEM- интеграция собственного и партнерского оборудования (Элес, ДеТеВе, PRC).
8. Координация усилий с Заказчиками (“Росатом”, “Газпромом”, “Роснефтью”, силовыми ведомства).
9. Сертификация оборудования и ПО во ФСТЭК и ФСБ.
10. Получен для оборудования “МиниКом” (DX-500, TETRA, DECT, Поток) от Минпромторга статус оборудования отечественного происхождения.

Отечественное оборудования “МиниКом DX-500” для построения систем открытой и защищенной связи АЭС

-отечественное происхождение оборудования (решение комиссии Минпромторга РФ):

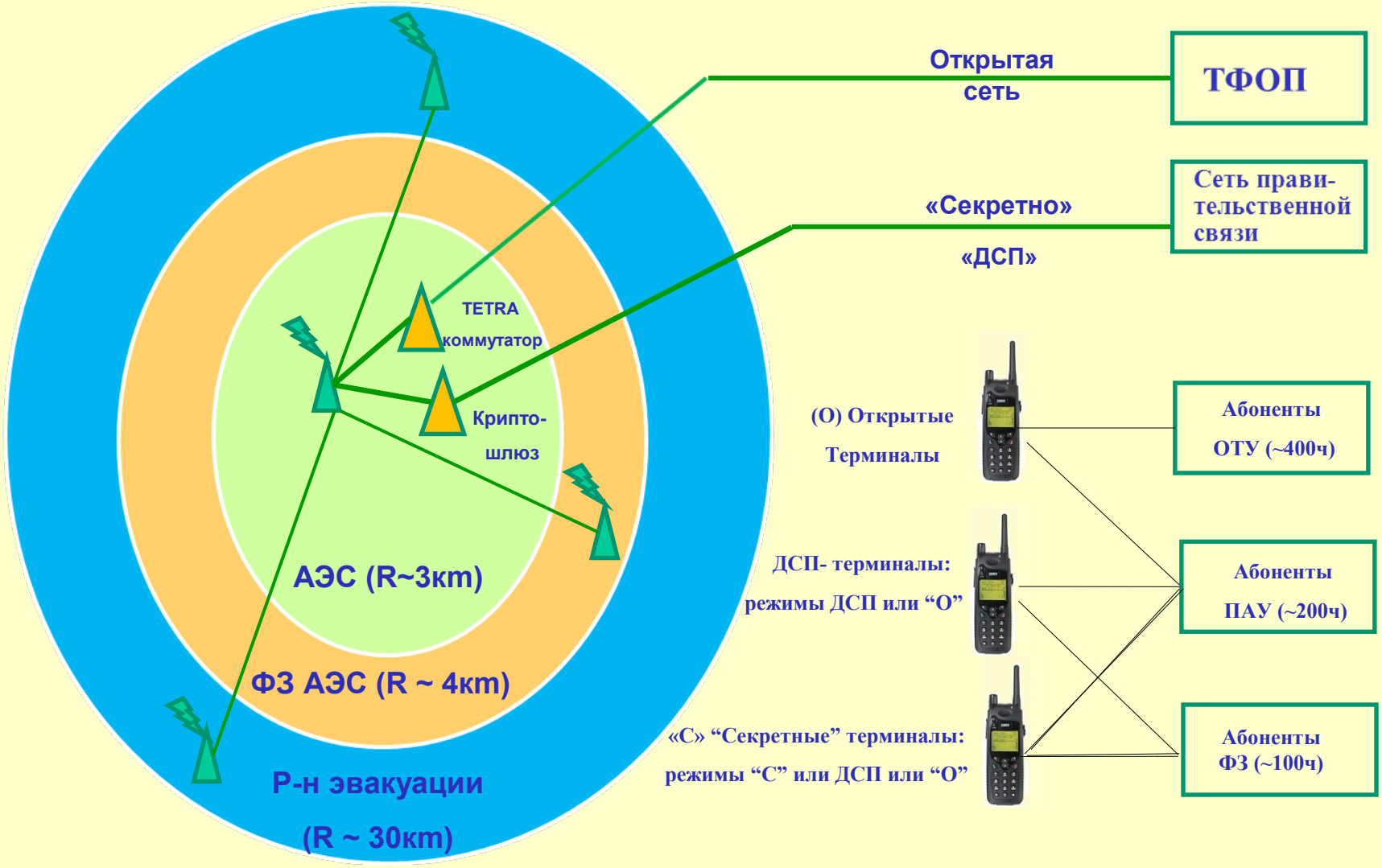
-наличие сертификатов ФСБ для обработки информации с грифами ДСП и С;

-возможность организовать на одной платформе группы абонентов конфиденциальной, открытой и защищенной связи;

-возможность выноса абонентов защищенной связи за пределы контролируемой территории;

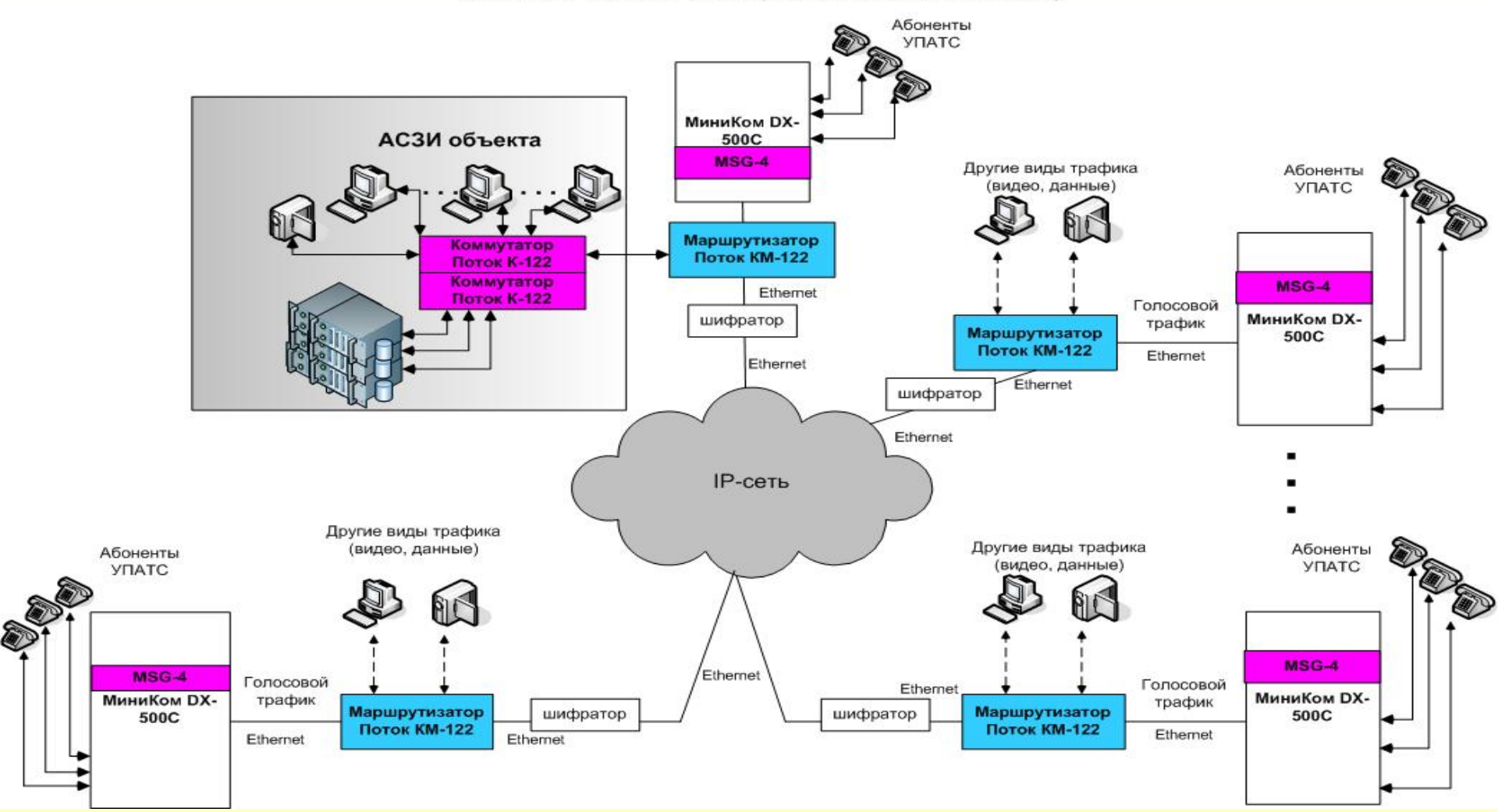
-минимизация внешних угроз (эмбарго, валютных рисков);

Единое МиниКом TETRA решение для радиосвязи: Оперативно-технологического управления (ОТУ), противо-аварийного управления(ПАУ) и управления физзащиты(УФЗ)=сертификат ФСБ



3-5 БС TETRA для покрытия ~700 абонентов АЭС (?DMR)

Применение коммутаторов МиниКом (Поток К-122 и КМ-122) для построения защищенной сети связи ведомства



1. **Разделение потоков управления и данных на коммутаторах Поток защищает от НСД и НДВ систему управления ИТ-системы.**
2. **Применимо для построения защищенных систем связи и оповещения, АСУТП и АСУП,**

4. Выводы

1. Применение импортного оборудования задало планку высокого качества, однако исторически сложилось негативное доминирование импортного оборудования (особенно- в радиосвязи и системах физзащиты).
2. Сейчас во всех нишах появилось конкурентное отечественное оборудование и происходит постепенное импортозамещение. Девальвация рубля является главной движущей силой импортозамещения.
3. Бесконтрольное применение импортного оборудования привело к новым угрозам в условиях санкций с точки зрения гарантий долговремменой техподдержки и поставки ЗИП. Спецустойчивости и инфобезопасности Необходимым условием компенсации угроз является развитие конкурентной отечественной промышленности. Многие проблемы импортозамещения являются междисциплинными.
4. Предложения:

-провести Отраслевое совещание по проблемам импортозамещения и инфобезопасности;

-провести анализ импортозависимости по ключевым видам оборудования;

-начать фоормировать программу импортозамещения на основе созданного НИАЭП электронного каталога ЕОНКОМ (Единый Отраслевой Каталог Оборудования и Материалов);

-внести в ИТТ/ТЗ на оборудование связи АЭС ввести требования по компенсации рисков применения импортного оборудования;

-признак отечественного происхождения телеком оборудования (в соответствии с квалификацией Минпромторга) должен обязательно учитываться при прочих равных условиях в ЕОСЗ;

-изменить редакцию РД 03-36 ГК "Росатом" по применению импортных комплектующих в части ограничений стран, объявивших санкции РФ:

-использовать опыт ГК “Информтехника” для разработки программы импортозамещения оборудования связи и АСУТП АЭС.