

Минкомсвязь
России



VI Уральский форум «Информационная безопасность банков»

Молот конфиденциальности в кредитно-финансовой сфере

Георгий Грицай,
Департамент регулирования радиочастот и сетей связи
Минкомсвязи России

Минкомсвязь
России



VI Уральский форум
«Информационная безопасность банков»

Молот конфиденциальности
в кредитно-финансовой сфере

...

и наковальня устойчивости
технических систем

Георгий Грицай,
Департамент регулирования радиочастот и сетей связи
Минкомсвязи России



Триады безопасности

- Конфиденциальность
- Целостность
- Доступность

- Целостность
- Устойчивость функционирования
- Безопасность





Целостность

Устойчивость функционирования

способность технической системы выполнять свои функции при отказе части компонентов в результате воздействия дестабилизирующих факторов и возвращаться в исходное состояние

Безопасность



Устойчивость по отношению к

- Внутренним дестабилизирующим факторам, определяется
 - **Надежностью** системы и ее компонентов (Reliability)
- Внешним дестабилизирующим факторам -
 - **Живучестью** системы и ее компонентов (Resiliency)



Требования к надежности и устойчивости к воздействиям технических и программных средств

- *Ех.* надежность аппаратуры, приборов, устройств и оборудования ВиВСТ...
- *Ех.* устойчивость (стойкость) к ЭМИ, механическим воздействиям, климатическим факторам...

Изм. № 1038

Для справок:
Экз. №

ГОСТ РВ.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ Ф

КОМПЛЕКСНАЯ СИСТЕМА
ОБЩИХ ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ

АППАРАТУРА, ПРИБОРЫ,
УСТРОЙСТВА И ОБОРУДОВАНИЕ
ВОЕННОГО НАЗНАЧЕНИЯ



Влияние на безопасность

- Реализация целевой функции на элементной базе ограниченной надежности
- P прохождения/обработки пакета данных/потока/сигнала, P искажения пакета данных/потока/сигнала
- P коммутации, P неверной коммутации
- Устойчивость к программно-математическим воздействиям
eq. защищенность от компьютерных атак



Устойчивость функционирования сети связи

- ГОСТ Р 53111-2005 Устойчивость функционирования сети связи общего пользования. Требования и методы проверки
 - ЦНИИС, ГНИИПТЗИ ФСТЭК России, ОАО МТТ
 - Категории потребителей и сетей, отказ, показатели надежности и живучести, мероприятия обеспечения, система восстановления

$$\rho_{ij} = E \left\{ \rho_{ij}^{\max} = 1 - \prod_{\forall \mu_{ij}^k \in m_{ij}} (1 - \rho_{ij}^k) \right\}$$



Устойчивость функционирования сети связи

- Мероприятия обеспечения
 - Объектовые, линейные
 - Сетевые - резервирование, выбор среды, топологии, сетевые присоединения, управление трафиком
- Задачи системы восстановления
 - Оперативные - 6...24/48 ч.;
восстановление ОНС/целостности
 - Среднесрочные - 10...30%% каналов связи/нагрузки
 - Долгосрочные



Устойчивость функционирования информационных систем

- *Ех.* Требования по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования
 - Приказ Минкомсвязи от 25.08.2009 №104 (ПП424)
 - Классы систем, показатели устойчивости, K готовности





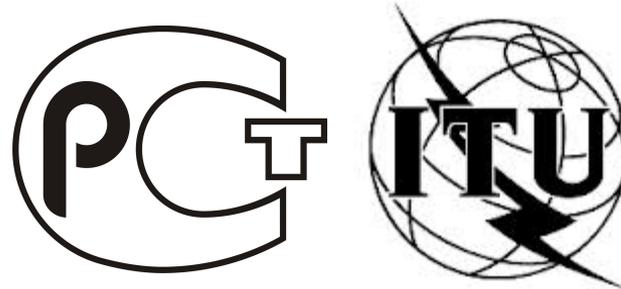
Управление непрерывностью бизнеса

- ГОСТ Р 53647.x Менеджмент непрерывности бизнеса / BS 25999:xxxx Business continuity management
- BS 25777:xxxx Information and communications technology continuity management / ISO 27031:xxxx
- СТО БР ИББС-1.0-2010 Обеспечении информационной безопасности организаций Банковской системы Российской Федерации. Общие положения - п.8.11. Требования к организации обеспечения непрерывности бизнеса и его восстановления после прерываний



Что не хватает Минкомсвязи?

- сквозной подход - от PDCA, RM до каталога мер
- “гармонизация” с документами TeleManagement Forum - NGOSS, eTOM и пр.
- ГОСТ Р, отраслевые НМД/НТД
- рекомендации ITU-T, обзоры ITU-D





Минкомсвязь
России

Наковальня устойчивости





Минкомсвязь
России

Наковальня устойчивости

**Законопроект о безопасности
критической информационной инфраструктуры
Российской Федерации**

2015 год - уже скоро!



Направления регулирования

- Требования безопасности
 - ГИС, СССН
 - АСУ ПТП КВО (кибер-кинетические системы), ТСС
 - ИС КИИ, ВСС
 - ИСОП КИИ, ССОП
- Обнаружение атак, реагирование на инциденты
 - СОПКА, ЦРКИ



Критическая информационная инфраструктура

совокупность элементов - ИС, ИТКС и СС, нарушение функционирования которых может повлечь негативные последствия в политической, экономической, социальной, экологической сферах, а также обороноспособности, обеспечения безопасности и правопорядка, управления и оказания государственных услуг

Банковские ИС, ИТКС филиальных сетей, сетей банкоматов, платежных терминалов...

Критерии категорирования опасности объектов

- **социальной значимости** (угроза жизни и здоровью людей, ухудшение обеспечения жизнедеятельности, транспорта, связи)
- **экономической значимости** (снижение экономических показателей, финансовые потери)
- **значимости по оказанию значительного объема государственных и социально значимых услуг** (объем неоказанных услуг и время их непредоставления)
- **значимости в реализации управленческой функции** (ущерб от потери управления или ухудшения качества управления в сфере, отрасли или секторе экономики или хозяйственной деятельности)
- **политической и экологической значимости, а также значимости для обороноспособности, безопасности государства и правопорядка**



Требования и система обеспечения безопасности КИИ

- к организационному обеспечению безопасности объекта КИИ
- к обеспечению безопасности ИС и ИТКС объекта КИИ
- к обеспечению безопасности АСУ ПТП объекта КИИ
- к СрЗИ и СОБИТ, применяемых для обеспечения безопасности объектов КИИ

Требования устанавливает уполномоченный ОГВ - ФСБ или ФСТЭК?

Дополнительные требования - отраслевые регуляторы, *ex.*: Банк России, Минкомсвязь...



Ответственность

Ч.3 ст.274 УК РФ - Нарушение правил эксплуатации средств обработки охраняемой информации, ИТКС и окончного оборудования, правил доступа к ИТКС, повлекшее ущерб КИИ или создавший угрозу его наступления

до 7 лет лишения свободы



В чем взаимный интерес Банка России и Минкомсвязи?

- Правительство – устанавливает порядок использования ресурсов ССОП для обеспечения связью объектов КИИ
- ФСБ России/ФСТЭК России и Минкомсвязь России - требования к СС, отнесенных объектам КИИ
- Требования к услугам связи, оказываемых отраслевым объектам КИИ, операторами СС, не отнесенных к объектам КИИ или имеющих меньшую категорию опасности - отраслевой регулятор и/или потребитель?

Согласованные требования или рекомендации

**Минкомсвязь
России**



VI Уральский форум «Информационная безопасность банков»

**Молот конфиденциальности
в кредитно-финансовой сфере**



**и наковальня устойчивости
технических систем**

Вопросы?

Георгий Грицай,
Департамент регулирования радиочастот и сетей связи
Минкомсвязи России