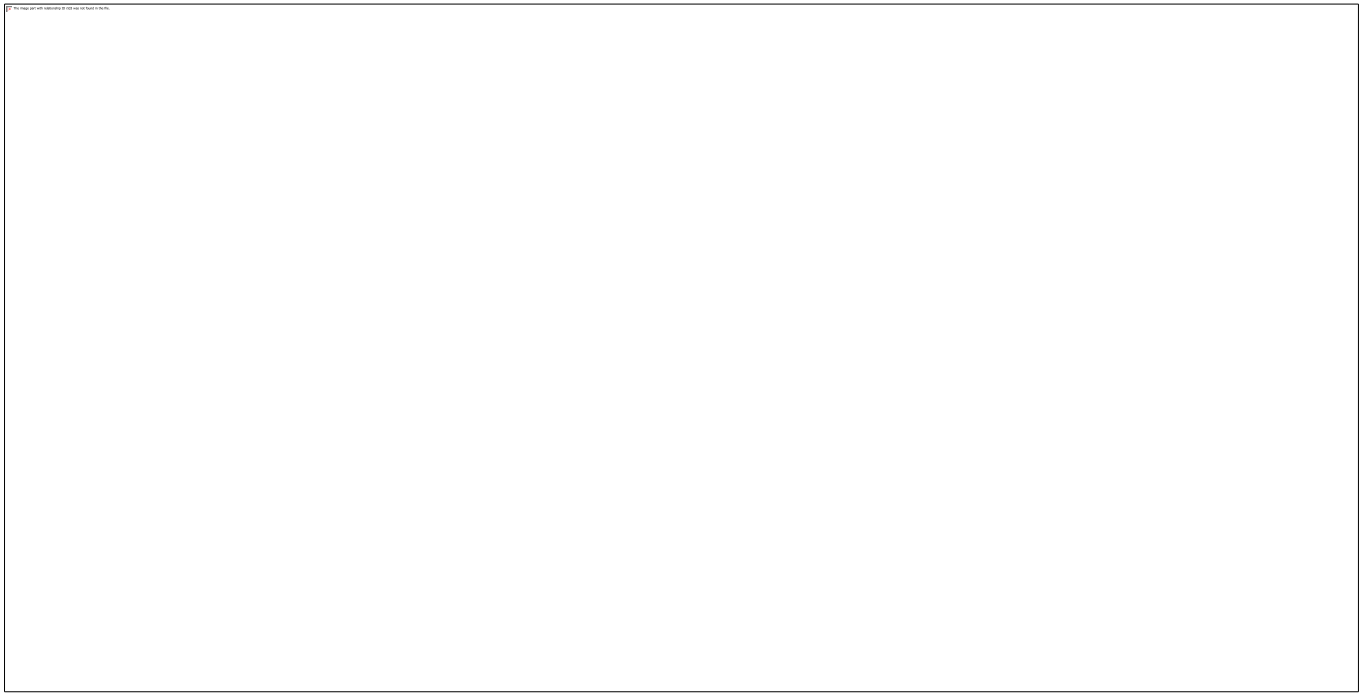
РИФ 2017
Лесные дали
19.04.2076

Инфраструктура Интернета в контексте регулирования жизненно важных услуг и критических информационных инфраструктур: обзор международного опыта



Олег Демидов
ПИР-Центр

Развитие регулирования в мире

- **Аргентина**
- **Германия**
- **КНР**
- **США**
- **Швеция**
- **Япония**

Инфраструктура Интернета в контексте КИИ/ЖВУ

- Инфраструктурные элементы глобальной системы уникальных идентификаторов Интернета (система УИИ), прежде всего инфраструктура DNS:
  - инфраструктурные элементы глобальной системы DNS: авторитативные корневые серверы DNS и их «зеркала»;
  - авторитативные серверы DNS, поддерживающие страновые и общие домены верхнего уровня;
  - нижестоящая по уровню иерархии DNS по отношению к авторитативным корневым серверам инфраструктура DNS-резолверов;

- Сетевая инфраструктура ключевых интернет-провайдеров: магистральные ВОЛС, инфраструктура энергоснабжения и проч., сетевое оборудование маршрутизации
- Инфраструктура, обеспечивающая связность и взаимодействие сетей различных операторов: точки обмена трафиком (IXPs), стыки инфраструктуры различных провайдеров (интерконнекты, телехаузы)

Общая картина

- **В международной практике НЕТ единого подхода к регулированию КИИ и единого понимания того, как соотносятся с КИИ сервисы и инфраструктура Интернета.**

- **НЕТ универсальной методологии, таксономии и системы критериев для категорирования и классификации КИИ**

- **Существующие подходы:**

1. (Япония, США и проч.) Объект регулирования - ИТ-инфраструктура КВО, категорирования и таксономии является производной по отношению к КВО. Интернет и сервисы ИТ-отрасли, не выделяются в отдельную категорию/сектор КВО.
2. (РФ) КИИ = отдельная категория объектов регулирования, но по системе критериев и таксономии производна по отношению к КВО. В ряде случаев понятие КИИ привязывается к АСУ ПТП КВО. Интернет + другие сети передачи данных относятся к КИИ, но в привязке к функционированию КВО.
3. (ЕС, Германия, Швеция) Регулирование КИИ параллельно регулированию КВО. ИТ+Интернет = отдельная сфера регулирования; вместо КИИ – жизненно важные услуги (ЖВУ) и критически важные услуги (КВУ).

Ключевые тенденции

- Вывод КИИ из элемента обеспечения функционирования КВО в самостоятельную сферу регулирования (КИИ – шире чем АСУ ПТП КВО)
- Инфраструктура и сервисы Интернета начинает выделяться в самостоятельный круг объектов регулирования; процесс не завершен
- Изменение взгляда на природу предмета регулирования: от защиты ***объектов*** инфраструктуры к обеспечению БСО (безопасность, стабильность, отказоустойчивость) ***услуг***, предоставляемых за счет такой инфраструктуры
- В рамках ИТ и Интернет отрасли: смена приоритетов от ***защиты*** и обеспечения ***безопасности*** к ***непрерывности бизнеса*** и обеспечению ***БСО***
- ЕС и государства-члены ЕС: смена целеполагания в регулировании – от обеспечения национальной безопасности за счет защиты КВО/КИИ – к гарантированному предоставлению населению ЖВУ/КВУ

Швеция

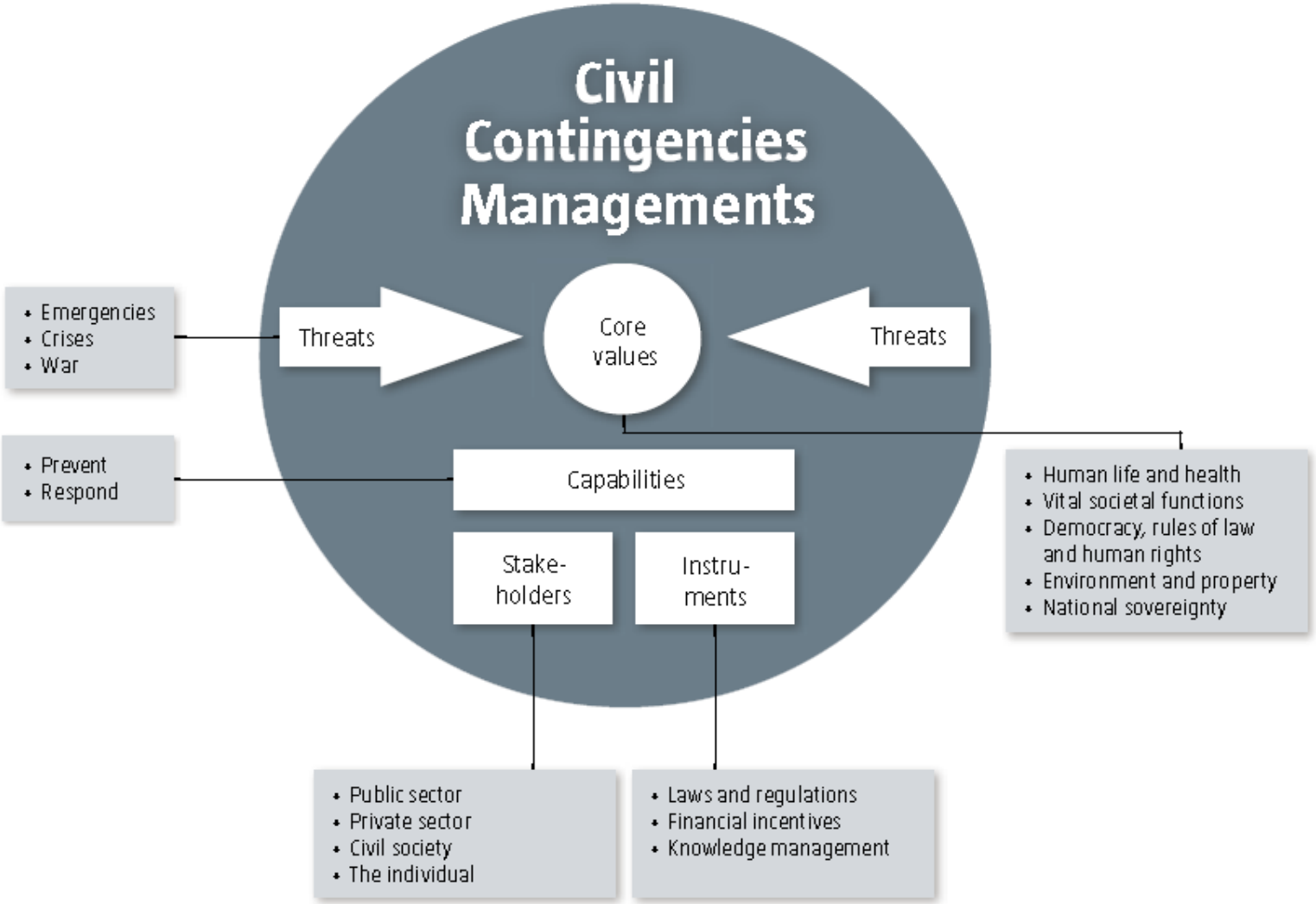
Безопасность КИ и жизненно важных общественных функций (Vital Social Functions, VSF)

- 2014 г.: План действий по защите жизненно важных общественных функций и КИ (до 2020 г.)
- 11 секторов КИ, синхронизированных с EPCIP
- Сектор информации и коммуникаций: мобильная и фиксированная телефонная связь, Интернет, радио-коммуникации, распределение почтовых отправлений информационное наполнение вебсайтов, социальные медиа и проч.

3 компонента подхода:

- Управление рисками (ISO 31000)
- Управление непрерывностью бизнеса (BCM, ISO 22301)
- Управление реагированием на инциденты и другие события

Швеция


Civil Contingencies Managements
Emergencies
Crises
War
Threats
Core values
Threats
Prevent
Respond
Capabilities
Stake-holders
Instru-ments
Human life and health
Vital societal functions
Democracy, rules of law and human rights
Environment and property
National sovereignty
Public sector
Private sector
Civil society
The individual
Laws and regulations
Financial incentives
Knowledge management

Швеция

Управление почты и телекоммуникаций (PTS): программа по сокращению уязвимостей сетей линий электропередачи и сервисов ведущих телеком-операторов

- обеспечение кризисной готовности и реагированию, включая направление по обеспечению устойчивости коммуникаций;
- каждому из 3 крупнейших национальных операторов поставлены 1600 малых резервных электрогенераторов, а также 10 мобильных базовых GSM-станций;
- расширение сетей ВОЛС, закупка узловое оборудование для соединительных сетей, усиление инфраструктуры сетей линий электропередачи в крупнейших города;
- обустройство защищенных подземных площадок для использования телеком-операторами для размещения и установки критического оборудования по себестоимости (коммутаторы, инфраструктура IXP, серверы DNS и проч.)
- 20 млн евро для содействия операторам в дальнейшем укреплении устойчивости и защищенности их инфраструктуры

ФРГ

2015 г.: внесение поправок в федеральное законодательство по ИБ через Акт об информационной безопасности (ITSG)

- Определение приоритетных секторов КИ
- Определение компетенций федеральных регуляторов по обеспечению ИБ КИ
- Выработка линейки требований по обеспечению ИБ и защите систем к операторам КИ

Апрель 2016 г.: Распоряжение Федерального управления по информационной безопасности (BSI) об определении круга операторов КИ (КВУ)

- Система метрик и количественных пороговых значений по всем видам КВУ
- «Правило 500 тыс.»: от услуг конкретного оператора должно зависеть не менее 500 тыс. чел. – критический порог, рассчитанный как доля от общего населения ФРГ (0,625% от 80 млн)

Классификация ФРГ и пороговые значения

РИФ 2017
Лесные дали
19.04.2076

№.	Категория критически важных услуг (КВУ)	Измеряемый критерий	Пороговое значение
1.	**Голосовая связь и передача данных**		
1.1	*Доступ*		
1.1.1	Сети локального доступа, обеспечивающие общедоступные услуги связи и передачи данных	Число клиентов	**100 000**
1.2.	*Передача голосового сигнала и данных*		
1.2.1	Передающие сети, поддерживающие общедоступные услуги передачи данных и доступа в Интернет (не входит пункт 1.1.1)	Кол-во пользователей соответствующей услуги	**100 000**
1.3	*Обмен трафика*		
1.3.1	Точки обмена трафиком (IXP)	Среднегодовое количество подключенных АС	**300 АС**
1.4.	*Управление DNS*		
1.4.1	Рекурсивные DNS-резолверы	Ежедневное количество DNS-запросов	**2 500 000**
1.4.2	Авторитативные серверы DNS	Кол-во доменов, для кот. сервер авторитативный	**250 000**

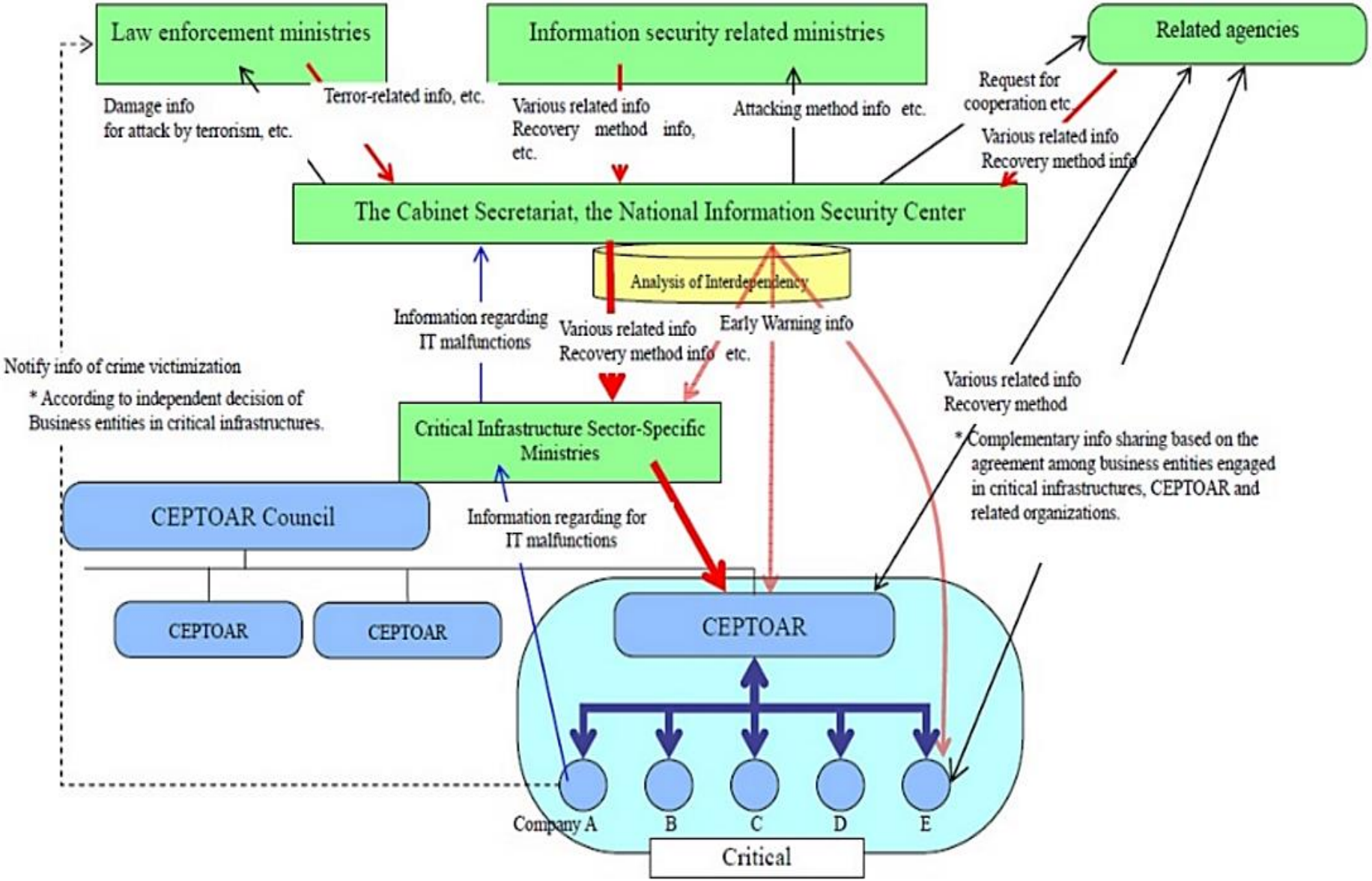
Классификация ФРГ и пороговые значения

РИФ 2017
Лесные дали
19.04.2076

№	Категория КВУ	Измеряемый критерий	Пороговое значение
2.	**Хранение и обработка данных**		
2.1	*Площадки хранения данных*		
2.1.1	Дата-центры	Законтрактованная мощность в МВт	**5 МВт**
2.2.	*Инфр-ра размещения и хранения данных*		
2.2.1	Серверные парки	Количество эксплуатируемых серверов	**25 000**
2.2.2	Сети доставки контента (CDN)	Объем передаваемых данных (ТБ в год)	**75 000 ТБ**
2.3.	*Выпуск цифровых сертификатов*		
2.3.1	Удостоверяющие центры	Кол-во выпущенных квалифицированных сертификатов	**500 000**
		Количество сертификатов для аутентификации общедоступного сервера (серверные серт-ты для веб-серверов, серверов ЭП, облачных сертификатов (включая серт-ты TLS/SSL)	**10 000**

Япония: опора на ГЧП

РИФ 2017
Лесные дали
19.04.2076



Япония

Система уведомления об инцидентах ИБ на объектах КИ

- Национальный центр реагирования на инциденты (National Incident Response Team, NIRT), являющийся частью Группы реагирования на компьютерные инциденты (CERT)

- Координационный центр японской группы реагирования на компьютерные инциденты (JCERT/cc) – первый в Японии CSIRT

- Кибер-отряд в Национальном полицейском агентстве – специализируется на борьбе с киберпреступностью, также оповещает операторов КИИ о случаях нестандартного использования Интернета в целях предотвращения террористических кибератак

- Министерство экономики и промышленности – взаимодействуя с JCERT/cc и IPA выпускает отчеты о компьютерных инцидентах, вирусных угрозах и причиненном ими ущербе.

Резюме

- Регулирование в сфере защиты КИИ / обеспечения БСО и целесообразно осуществлять в рамках комплексного межсекторального подхода, а не для Интернет-сектора по отдельности

- Повышенное внимание к потребностям населения к гарантированном предоставлению ЖВУ/КВУ, обеспечиваемых за счет КИИ

- Переход от классового подхода к определению перечня КИИ к индивидуальному. Разработка/обновление системы метрик, количественных параметров и пороговых значений для категорирования и формирования перечня/реестра операторов КИИ (востребован для изучения опыт ФРГ).

- Цель подхода – корректное и обоснованное определение операторами КИИ в зависимости от прямого охвата населения их услугами + выведение из-под повышенных требований и административного бремени малых операторов и иных субъектов ИТ-отрасли

Резюме

- Более активная локализация, адаптация и инкорпорирование в регуляторные подходы и практики операторов международных стандартов БСО и непрерывности бизнеса (business continuity)

- Инвестирование ресурсов и создание благоприятной регуляторной среды для развития системы государственно-частных партнерств (ГЧП) для обмена информацией, опытом, лучшими практиками и экспертизой по защите и обеспечению устойчивости КИИ

- Стимулирование развития системы отраслевых/секторальных CSIRT и CERT в ИТ-отрасли и Интернет-секторе с ведущей ролью частных операторов связи с целью более эффективного и гибкого предупреждения, предотвращения, реагирования и восстановления после инцидентов на КИИ (CII-CERT, Telecom-CERT) + более активная интеграция национальных групп реагирования на инциденты на КИИ в международные сети и ассоциации CERT/CSIRT (опыт ЕС, США, Японии)

Спасибо за внимание!