Особенности обеспечения безопасности критической инфраструктуры в других странах

Алексей Лукацкий
Бизнес-консультант по безопасности

Обязательность

Обязательность требований по защите КИИ в разных странах

- США

  NERC CIP – обязательно

  USNRC – обязательно

  NIST CSF - добровольно

- ЕС

  Директива NIS – обязательно с 18 мая 2018 (транзитный период на 2 года)

- Германия

  IT Security Act – обязательно с 25 июля 2015 (транзитный период на 2 года)

Обязательность требований по защите КИИ в разных странах

- Великобритания

  CPNI Passport to Good Security – добровольно

- Франция

  Military Programming Act – обязательно

  Указ от 10 и 17 июня 2016 – обязательно

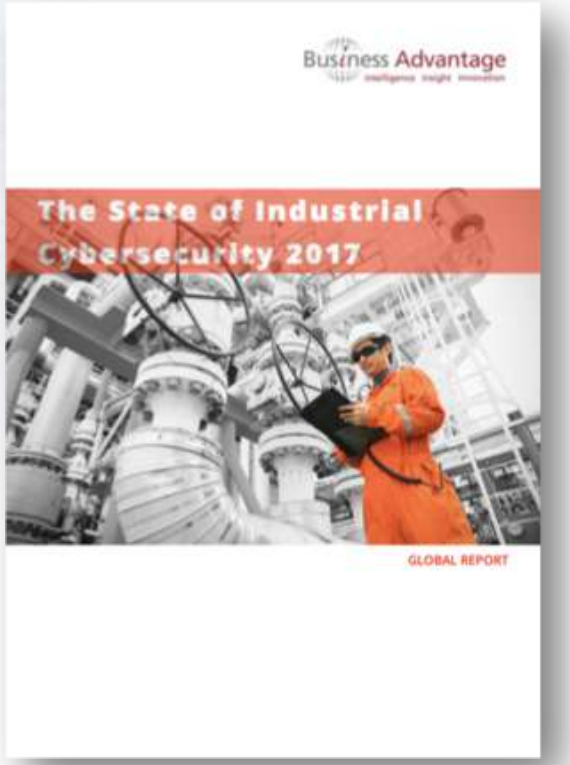
  Указ от 11 августа 2016 - обязательно

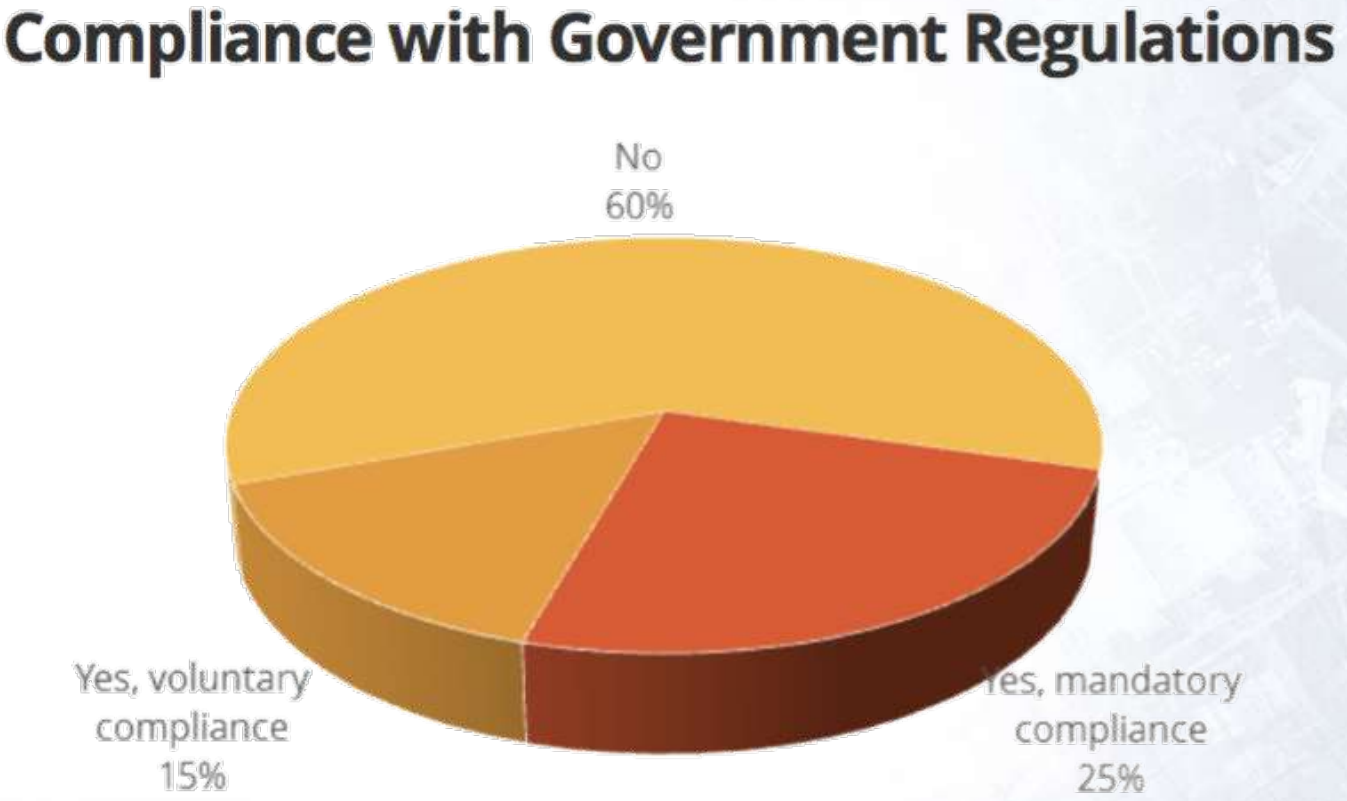
- Китай

  Cyber Security Act – обязательно с 1 июня 2017

cisco

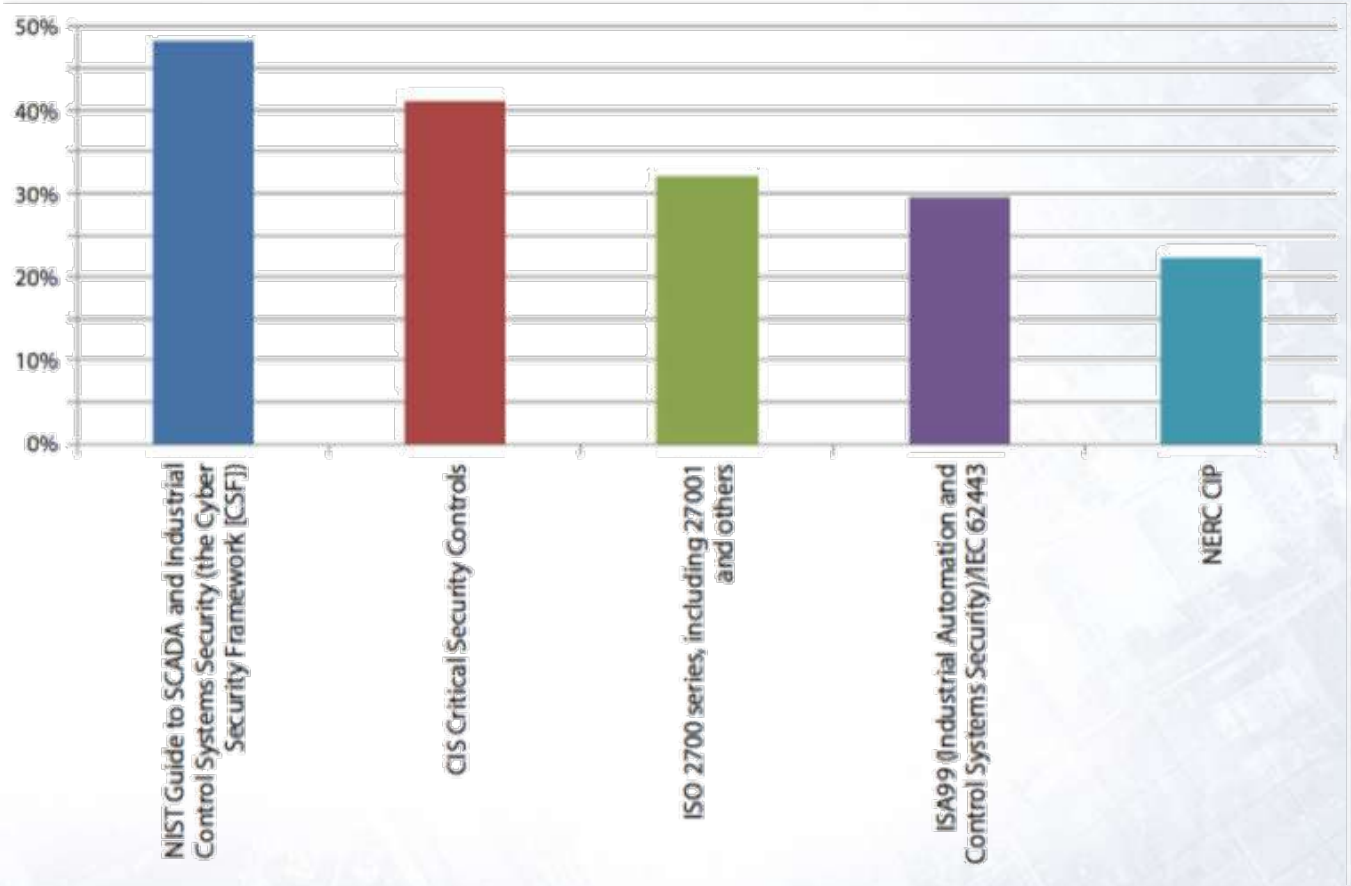
Обязательность требований по защите КИИ в разных странах





CISCO

Обязательность требований по защите КИИ в США

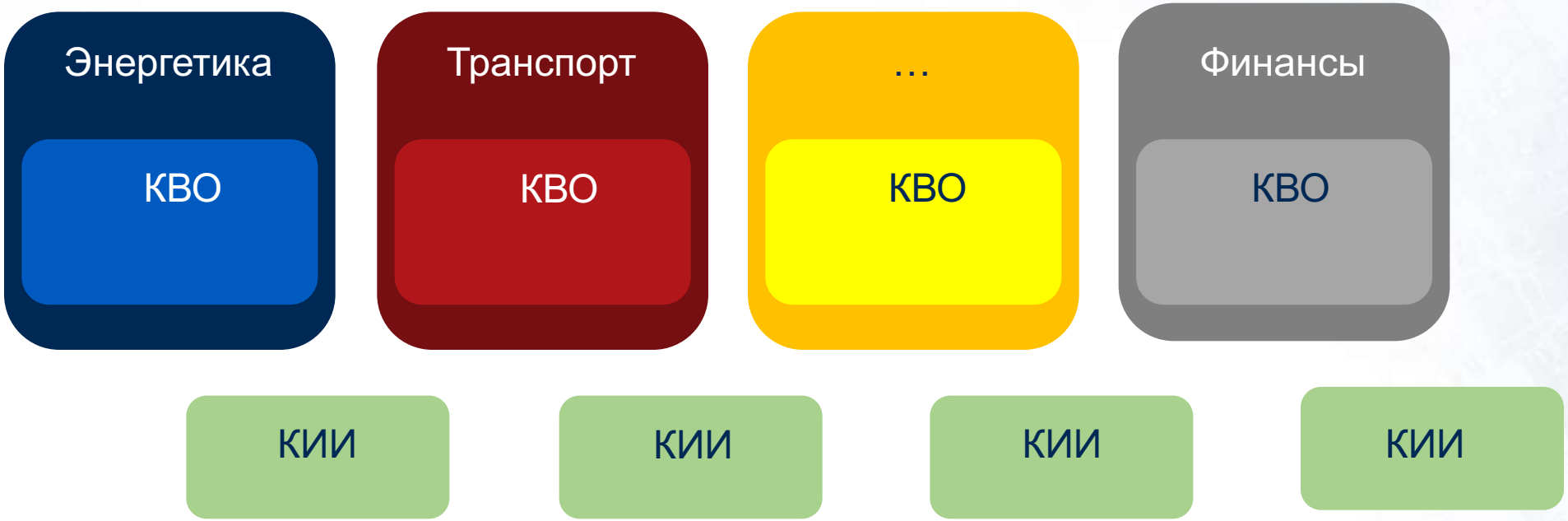


CISCO

КИ vs КИИ vs КВО

Критическая инфраструктура и КИИ

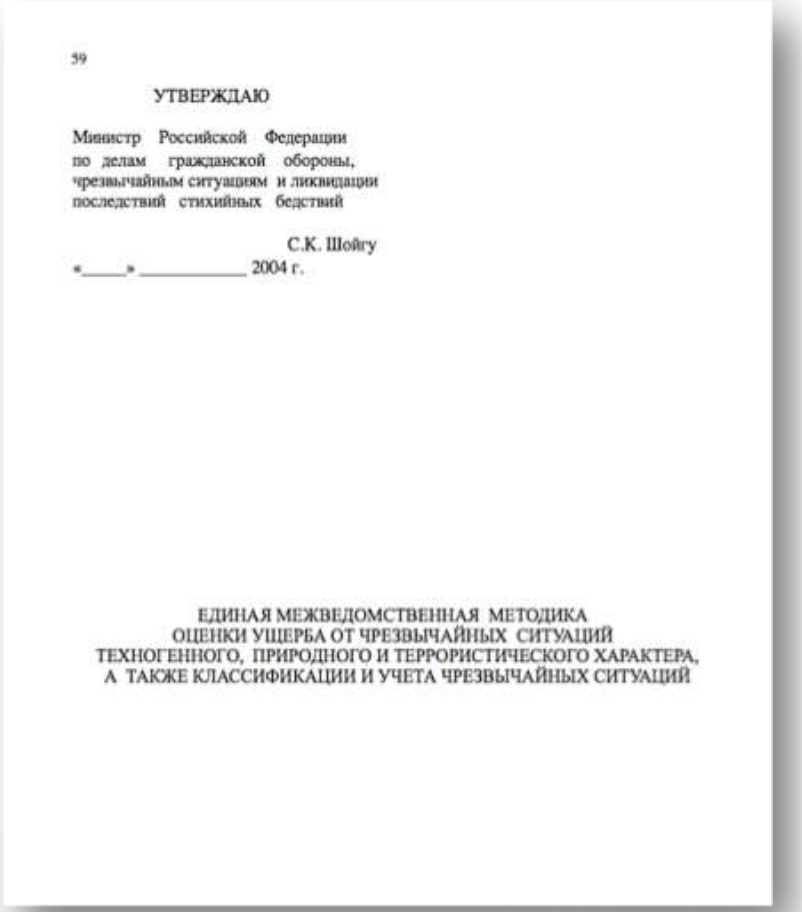
Но критическая инфраструктура ≠ КВО



- Осознанное разнесение КИИ и КВО

cisco

КВО никак не связаны с КИИ



59

УТВЕРЖДАЮ

Министр Российской Федерации
по делам гражданской обороны,
чрезвычайным ситуациям и ликвидации
последствий стихийных бедствий

С.К. Шойгу

«_____» _____ 2004 г.

ЕДИНАЯ МЕЖВЕДОМСТВЕННАЯ МЕТОДИКА
ОЦЕНКИ УЩЕРБА ОТ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ
ТЕХНОГЕННОГО, ПРИРОДНОГО И ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА,
А ТАКЖЕ КЛАССИФИКАЦИИ И УЧЕТА ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

- Различные методики и документы по КВО, опасным объектам, антитеррору, стратегически важным объектам и т.п.

Категорирование

Общие замечания

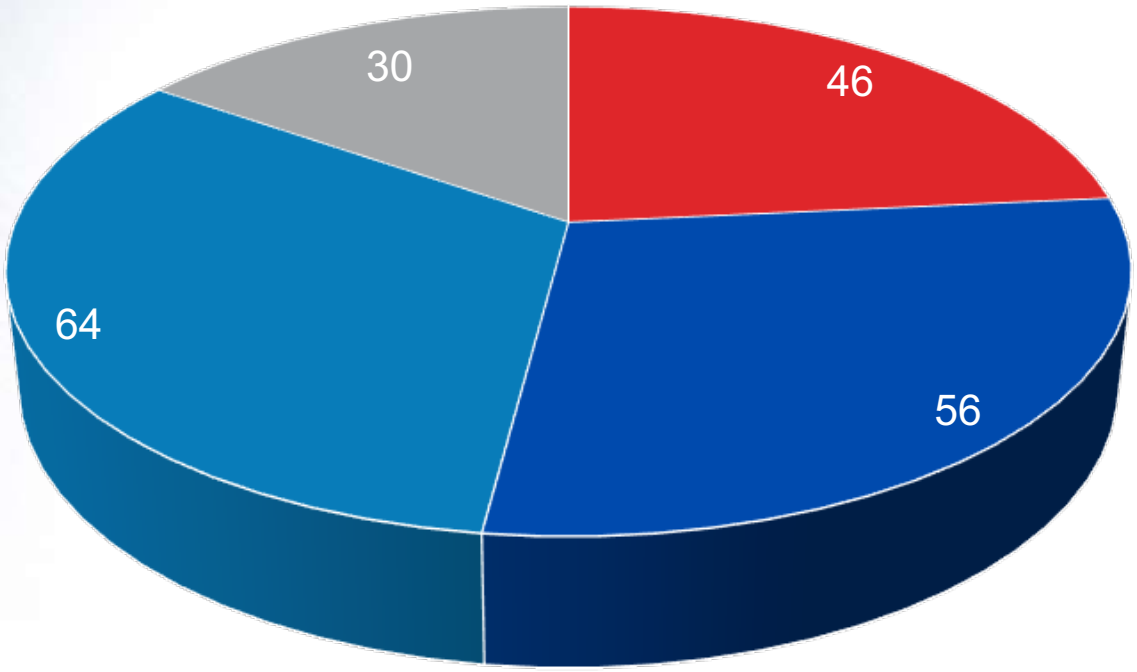
- Во многих странах конкретные показатели критериев являются непубличной, а иногда и конфиденциальной информацией
- Конкретные показатели критериев меняются от страны к стране и зависят от сектора с критической инфраструктурой
- В большинстве стран (например, США) за категорирование отвечают уполномоченные органы, а не сами субъекты

Общие замечания

- Во многих странах информационные системы (исключая самостоятельный сектор «ИТ и связь»), как и иные элементы критической инфраструктуры, явно не выделяют и не описывают их влияние на критичность
- В некоторых странах вообще нет конкретных показателей критериев категорирования – достаточно «попасть» в соответствующий сектор или отрасль

ГосСОПКА

Государственный CERT



- Нифига не делают
- Начали активности
- Имеют стратегию, регулятора и CSIRT
- Еще и государственно-частное партнерство реализуют и межведомственное взаимодействие есть

- Большинство стран мира только начинают работы по выстраиванию стратегии кибербезопасности на национальном уровне
- Государственный CERT имеют только половину государств, а сфокусированный на КИИ и того меньше

Основы регулирования ГосСОПКА

- Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации

  Утверждены Президентом РФ 3 февраля 2012 г. №803

- Указ Президента РФ от 15 января 2013 года № 31с
- Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

  №К 1274 от 12 декабря 2014г.

- Указ Президента РФ от 22 мая 2015 года №260
- ФЗ-187 «О безопасности КИИ РФ»

cisco

Что означает присоединение к ГосСОПКЕ?

- Информирование об инцидентах на всех объектах КИИ вашего центра ГосСОПКИ
- Содействие сотрудникам ФСБ в деятельности по реагированию на инциденты
- Выполнять требования по установке и эксплуатации средств ГосСОПКИ на объектах КИИ (если устанавливаются)

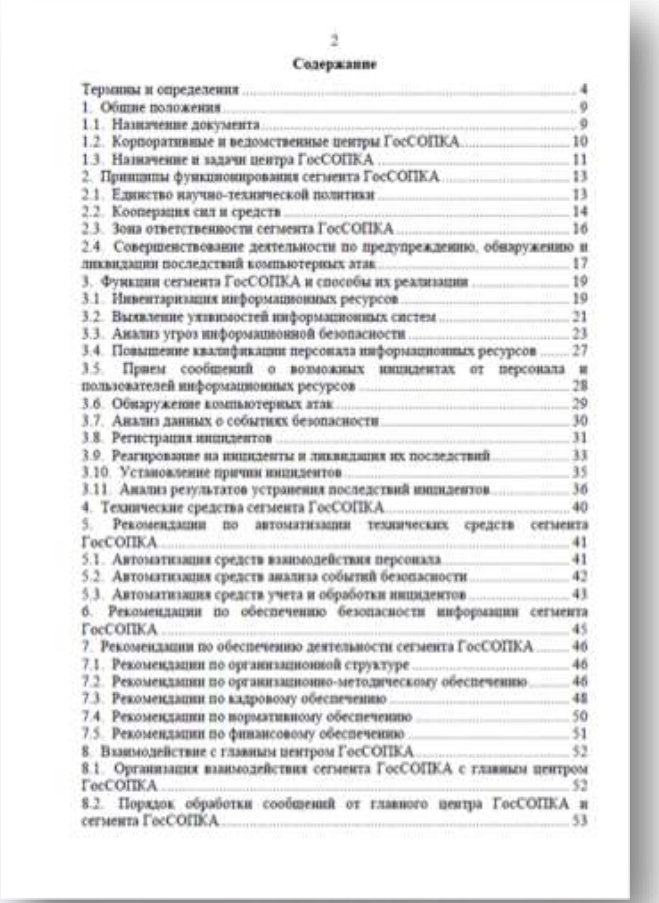
cisco

Методические рекомендации по созданию центров ГосСОПКИ

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ И СПЕЦИАЛЬНОЙ СВЯЗИ

Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

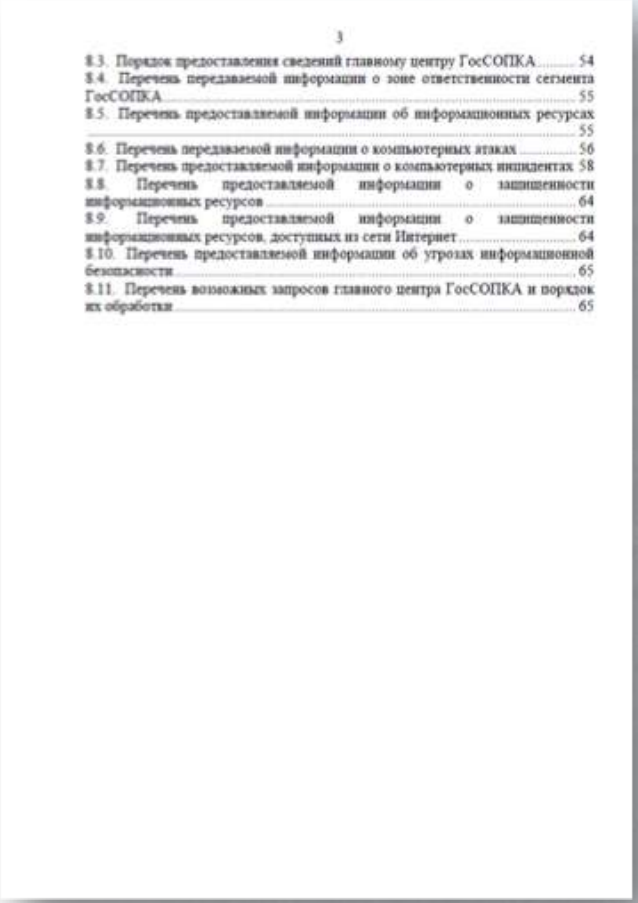
Москва, 2016



2

Содержание

Термины и определения ... 4
1. Общие положения ... 9
1.1. Назначение документа ... 9
1.2. Корпоративные и ведомственные центры ГосСОПКА ... 10
1.3. Назначение и задачи центра ГосСОПКА ... 11
2. Принципы функционирования сегмента ГосСОПКА ... 13
2.1. Единство научно-технической политики ... 13
2.2. Кооперация сил и средств ... 14
2.3. Зона ответственности сегмента ГосСОПКА ... 16
2.4. Совершенствование деятельности по предупреждению, обнаружению и ликвидации последствий компьютерных атак ... 17
3. Функции сегмента ГосСОПКА и способы их реализации ... 19
3.1. Инвентаризация информационных ресурсов ... 19
3.2. Выявление уязвимостей информационных систем ... 21
3.3. Анализ угроз информационной безопасности ... 23
3.4. Повышение квалификации персонала информационных ресурсов ... 27
3.5. Прием сообщений о возможных инцидентах от персонала и пользователей информационных ресурсов ... 28
3.6. Обнаружение компьютерных атак ... 29
3.7. Анализ данных о событиях безопасности ... 30
3.8. Регистрация инцидентов ... 31
3.9. Реагирование на инциденты и ликвидация их последствий ... 33
3.10. Установление причин инцидентов ... 35
3.11. Анализ результатов устранения последствий инцидентов ... 36
4. Технические средства сегмента ГосСОПКА ... 40
5. Рекомендации по автоматизации технических средств сегмента ГосСОПКА ... 41
5.1. Автоматизация средств взаимодействия персонала ... 41
5.2. Автоматизация средств анализа событий безопасности ... 42
5.3. Автоматизация средств учета и обработки инцидентов ... 43
6. Рекомендации по обеспечению безопасности информации сегмента ГосСОПКА ... 45
7. Рекомендации по обеспечению деятельности сегмента ГосСОПКА ... 46
7.1. Рекомендации по организационной структуре ... 46
7.2. Рекомендации по организационно-методическому обеспечению ... 46
7.3. Рекомендации по кадровому обеспечению ... 48
7.4. Рекомендации по нормативному обеспечению ... 50
7.5. Рекомендации по финансовому обеспечению ... 51
8. Взаимодействие с главным центром ГосСОПКА ... 52
8.1. Организация взаимодействия сегмента ГосСОПКА с главным центром ГосСОПКА ... 52
8.2. Порядок обработки сообщений от главного центра ГосСОПКА и сегмента ГосСОПКА ... 53



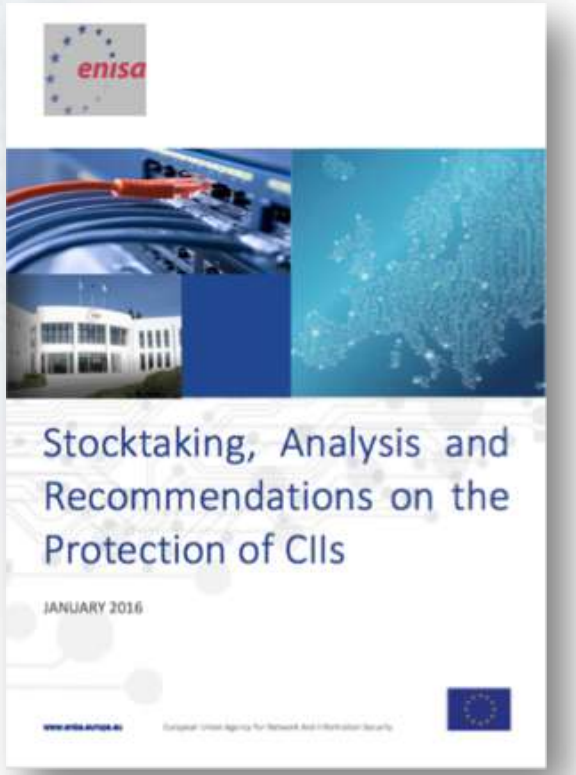
3

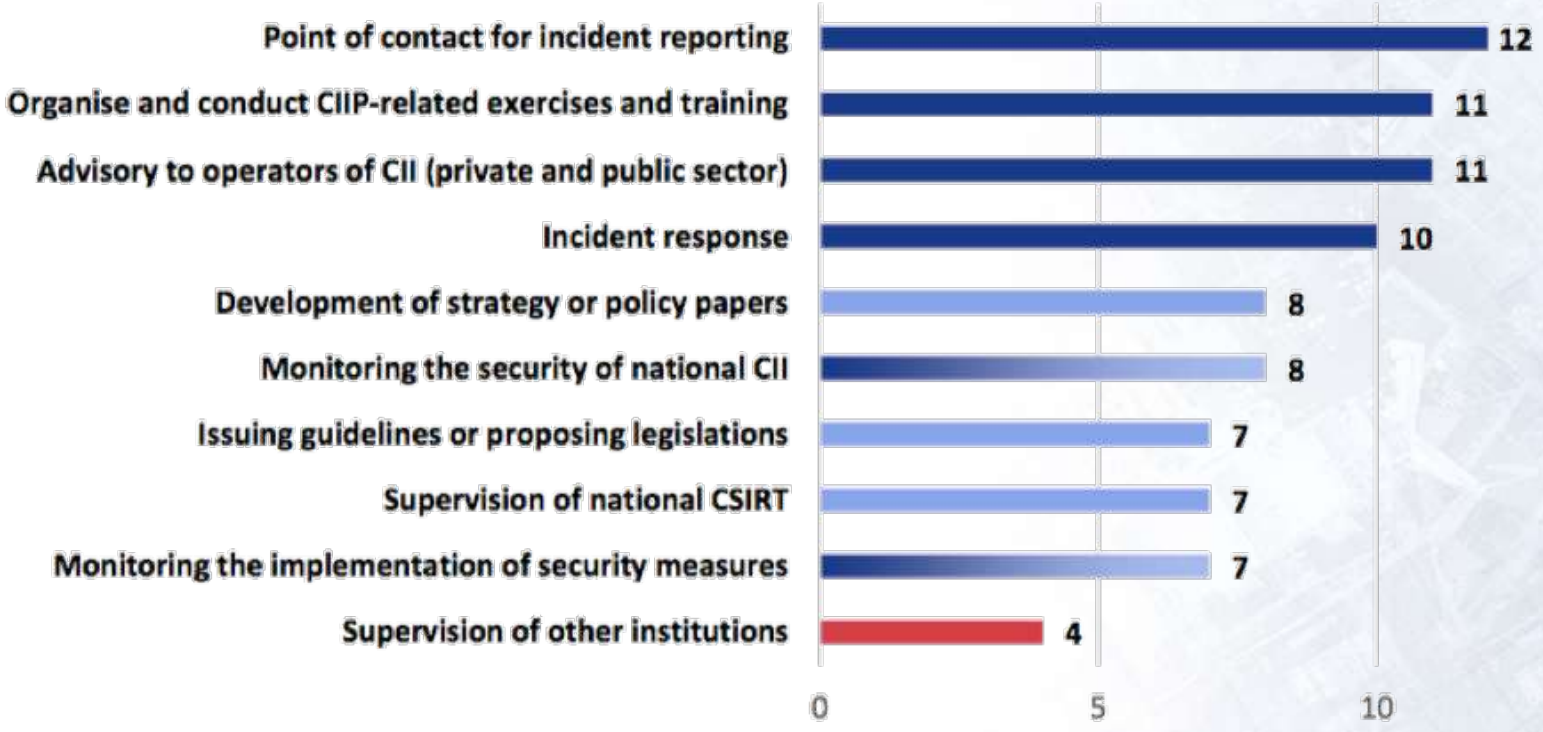
8.3. Порядок предоставления сведений главному центру ГосСОПКА ... 54
8.4. Перечень передаваемой информации о зоне ответственности сегмента ГосСОПКА ... 55
8.5. Перечень предоставляемой информации об информационных ресурсах ... 55
8.6. Перечень передаваемой информации о компьютерных атаках ... 56
8.7. Перечень предоставляемой информации о компьютерных инцидентах 58
8.8. Перечень предоставляемой информации о защищенности информационных ресурсов ... 64
8.9. Перечень предоставляемой информации о защищенности информационных ресурсов, доступных из сети Интернет ... 64
8.10. Перечень предоставляемой информации об угрозах информационной безопасности ... 65
8.11. Перечень возможных запросов главного центра ГосСОПКА и порядок их обработки ... 65

cisco

Ответственность регуляторов

Роли и задачи регуляторов по безопасности КИИ в ЕС





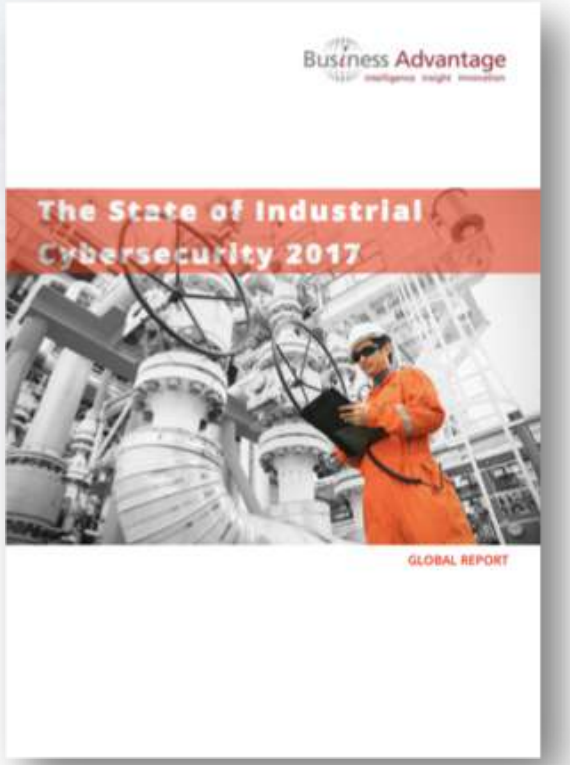
CISCO

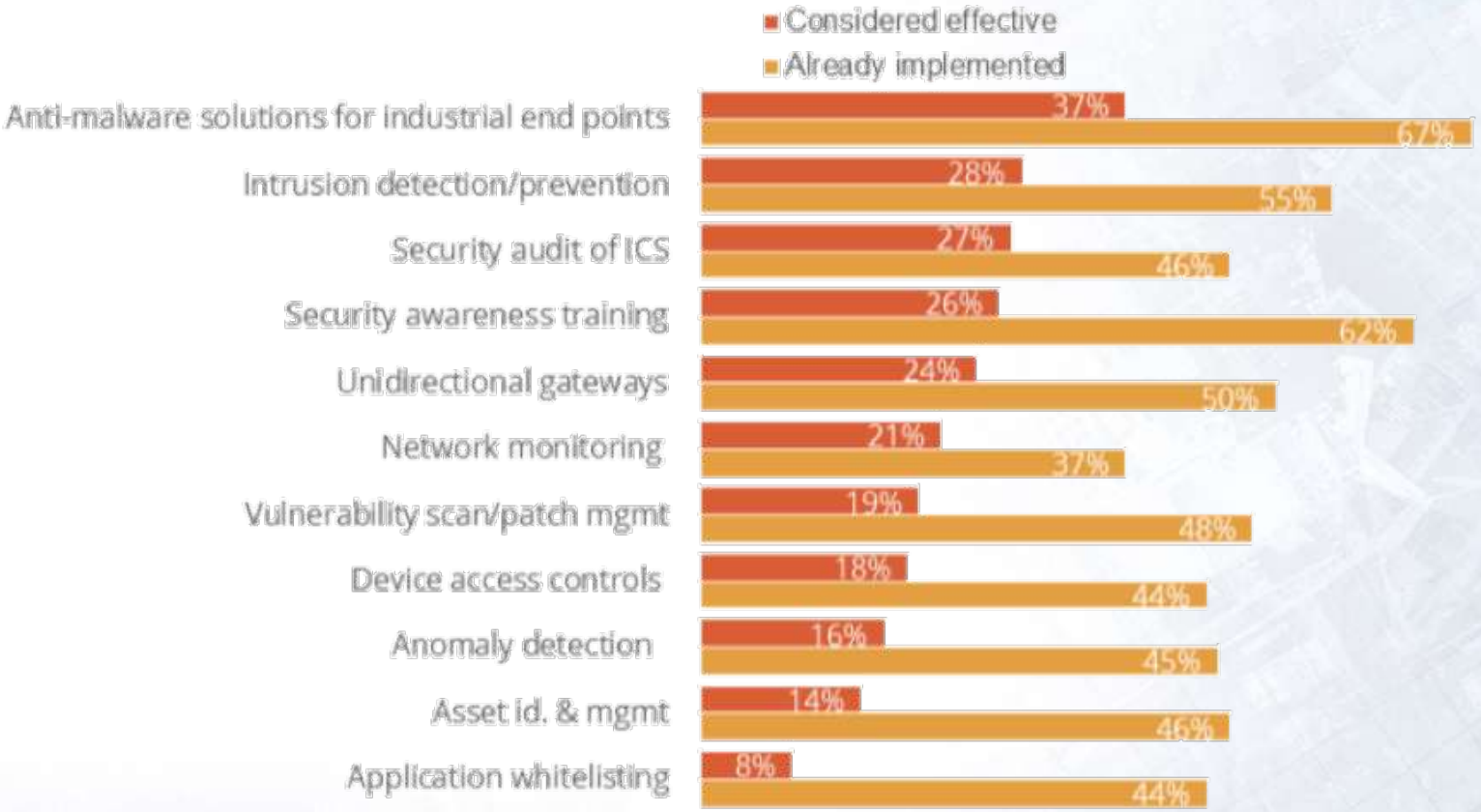
Требования по ИБ

Отсутствие единства требований

Выбор средств защиты и оценка соответствия

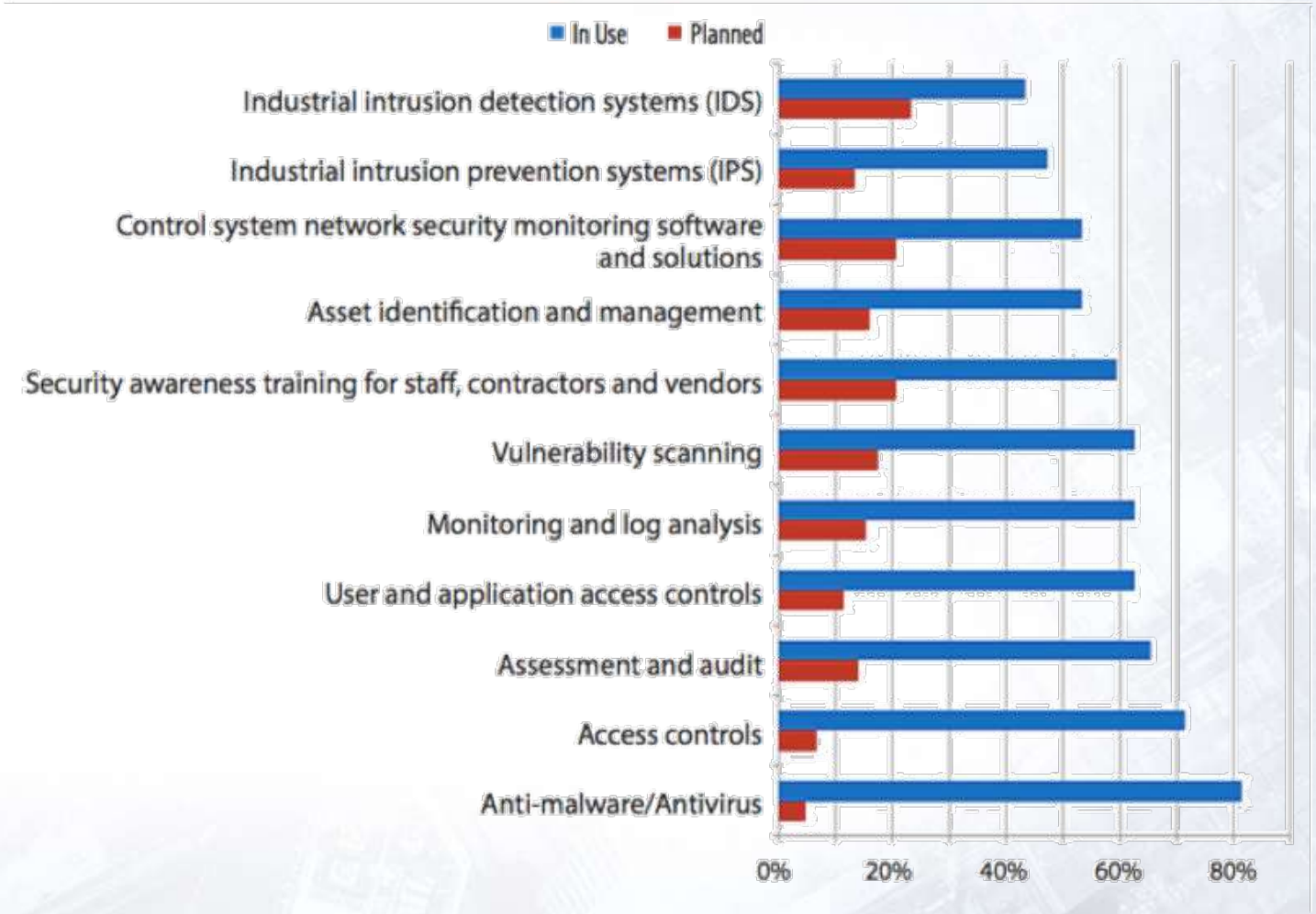
Несмотря на гибкость выбора защитных мер используемый набор невелик





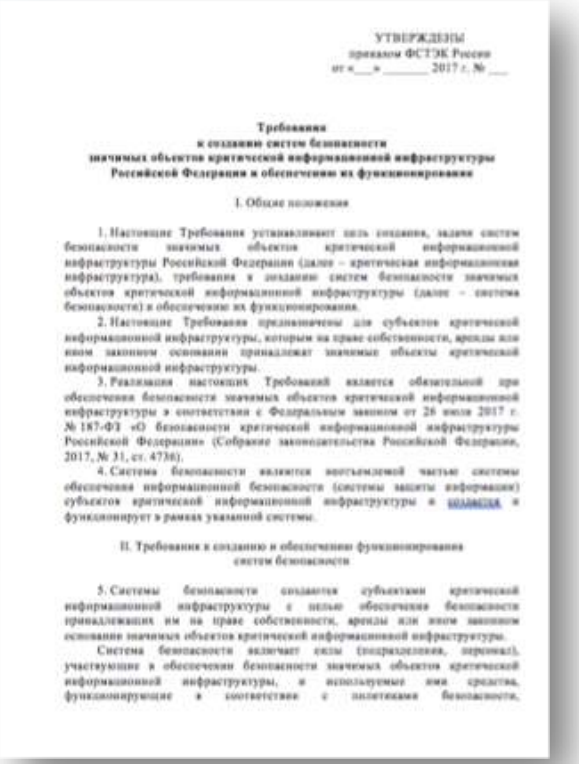
CISCO

Несмотря на гибкость выбора защитных мер используемый набор невелик



CISCO

Нюансы выбора средств защиты



УТВЕРЖДЕНЫ
приказом ФСТЭК России
от «___» _____ 2017 г. № ___

Требования
к созданию систем безопасности
значимых объектов критической информационной инфраструктуры
Российской Федерации и обеспечению их функционирования

I. Общие положения

1. Настоящие Требования устанавливают цель создания, задачи систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (далее – критическая информационная инфраструктура), требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры (далее – система безопасности) и обеспечению их функционирования.

2. Настоящие Требования предназначены для субъектов критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры.

3. Реализация настоящих Требований является обязательной при обеспечении безопасности значимых объектов критической информационной инфраструктуры в соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736).

4. Система безопасности является неотъемлемой частью системы обеспечения информационной безопасности (системы защиты информации) субъектов критической информационной инфраструктуры и создается и функционирует в рамках указанной системы.

II. Требования к созданию и обеспечению функционирования систем безопасности

5. Системы безопасности создаются субъектами критической информационной инфраструктуры с целью обеспечения безопасности принадлежащих им на праве собственности, аренды или ином законном основании значимых объектов критической информационной инфраструктуры.

Система безопасности включает силы (подразделения, персонал), участвующие в обеспечении безопасности значимых объектов критической информационной инфраструктуры, и используемые ими средства, функционирующие в соответствии с политиками безопасности,

- Оценка соответствия в форме обязательной сертификации, испытаний или приемки
- Обслуживание объекта КИИ или обеспечение его безопасности осуществляется «российской организацией»
- Средства защиты обеспечены поддержкой со стороны «российской организации», не имеют неконтролируемого обновления или управления из-за рубежа, не осуществляют несанкционированную передачу информации разработчику

cisco

Гостайна

Гостайна в КИИ?

- К гостайне относятся сведения о мерах по обеспечению безопасности КИИ и о состоянии ее защищенности от компьютерных атак
- Должен быть принят нормативный акт, устанавливающий конкретный перечень сведений, относимых к гостайне
- Это могут быть ТЗ, ТП, информация о госзакупках и тендерах, применяемые меры/средства защиты, результаты аудитов/пентестов и др.
- Речь не идет о необходимости иметь сертификат на ГТ у средств защиты КИИ

Лицензирование

Лицензирование деятельности по мониторингу

- В соответствие с ПП-541 от 15.06.2016 услуги по мониторингу ИБ средств и систем информатизации подлежат лицензированию
- Лицензируется деятельность для внешних нужд (коммерческие SOC, холдинговые структуры и т.п.)
- Требования к SOC от ФСТЭК не всегда коррелируют с требованиями ФСБ к центрам ГосСОПКИ

cisco

Технические средства лицензируемого SOC

- Система анализа защищенности
- Песочница
- Система Threat Intelligence
- SIEM
- Система управления инцидентами ИБ
- Средство защиты каналов связи (до SOC от контролируемых средств защиты)
- ИС для мониторинга (сам SOC) – аттестат на ГИС1

Красным отмечены средства, отсутствующие в требованиях ФСБ

Киберучения

Киберучения

- NSA Cyber Defense Exercise (CDX)
- Locked Shield
- Red Flag
- Cyber Shield
- Quantum Dawn
- Cyber Storm
- Cyber Guard
- Cyber Europe
- @tomic
- GridEx

Государственно-частное партнерство

Государственно-частное партнерство

- Привлечение частного сектора, который в 80% случаев и владеет КИИ, к обсуждению вопросов регулирования и обмена информацией об угрозах

  UP KRITIS или Alliance for Cyber Security в Германии, SAMFI в Швеции

- Взаимодействие частных и государственных CERTов

  CERT-Verbund в Германии

- Взаимодействие преимущественно в форме ГПЧ или рабочих групп

Выводы

Выводы

- В большинстве стран требования по ИБ КИИ носят преимущественно добровольный характер с постепенным сдвигом в сторону обязательности
- Категорирование объектов КИИ обычно осуществляется государством, а не субъектами
- Постепенно создаются государственные CERTы, но только как центры обмена информацией
- Лицензирования и сертификации по ИБ КИИ нет практически нигде; как и гостайны в КИИ
- Взвешенный подход к выбору защитных мер
- Активное использование киберучений
- Рост государственно-частного партнерства

Спасибо!

alukatsk@cisco.com

cisco