# Законопроект по безопасности критической инфраструктуры

Алексей Лукацкий
Бизнес-консультант по безопасности

19 апреля 2017

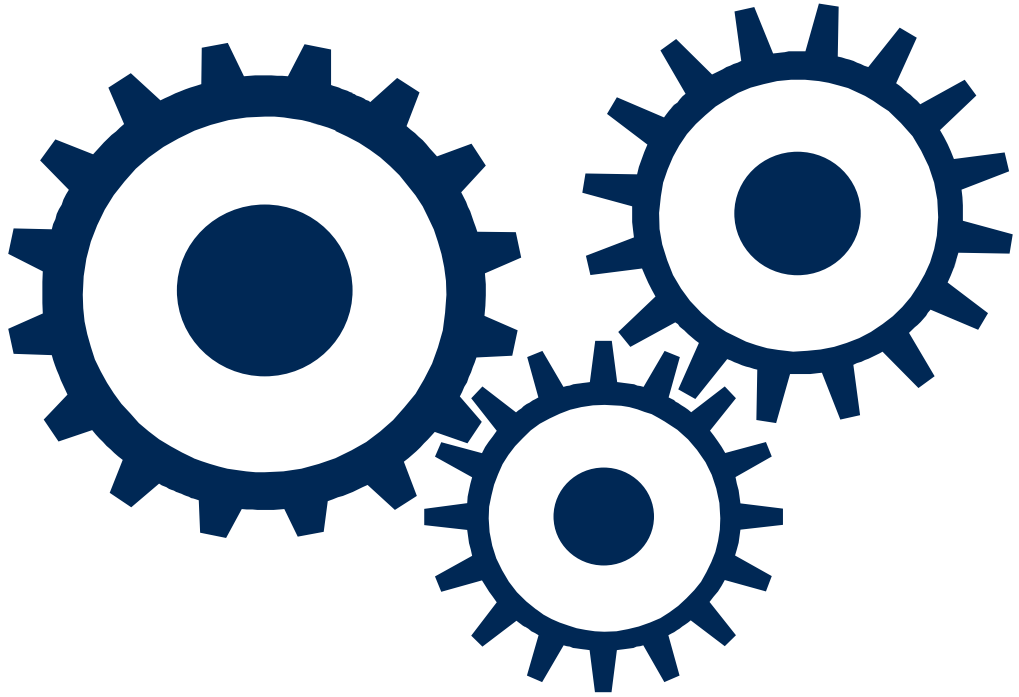
# Законопроект

## Декабрь 2016

Внесение в ГосДуму

- Категорирование объектов КИИ
- Новый регулятор (ФСТЭК или ФСБ)
- Присоединение к сетям электросвязи
- Выполнение требований ФСБ по реагированию на инциденты
- Присоединение к ГосСОПКЕ

# Кто будет отнесен к КИИ?



## Отсутствие

единообразия в терминологии в основных нормативных правовых актах – законопроекте о безопасности КИИ, основах госполитики в области безопасности АСУ ТП, приказе ФСТЭК №31 и документах МинЭнерго и МЧС

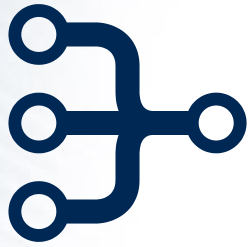
cisco

# Что такое критическая информационная инфраструктура?

| 2013 | 2014 | 2016 |
| --- | --- | --- |
| • Совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, а также информационных систем и сетей связи, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка | • Совокупность информационных систем, информационно-телекоммуникационных сетей и сетей связи, прекращение или нарушение которых может повлечь отрицательные (негативные) последствия в политической, социальной, экономической, экологической сферах, а также в сфере обороноспособности, обеспечения безопасности государства и правопорядка, управления и предоставления государственных услуг | • Совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой |

Законопроект «О безопасности КИИ»

# Отдельные категории субъектов КИИ



## Операторы связи

подпадают под регулирование Министерства связи и массовых коммуникаций, которое разработает требования по защите по согласованию с ФОИВ по безопасности КИИ и с ФСБ в части ГосСОПКИ

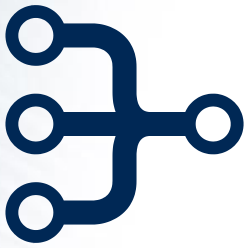
## Финансовые организации

**возможно**, перейдут под регулирование Банка России с его множеством нормативных документов по защите информации (пока на уровне предложений)

cisco

# Объекты КИИ образца 2016-го года

# От чего зависит категория объекта КИИ



## Субъекты КИИ или лицензиаты ФСТЭК

на основании установленных критериев и в соответствии с утвержденными показателями этих критериев, осуществляют отнесение принадлежащих им на праве собственности или ином законном основании объектов КИИ к установленным категориям

## Критерии

- социальной значимости (теперь включает госуслуги)
- политической значимости
- экономической значимости
- экологической значимости
- значимости для обеспечения обороноспособности, безопасности государства и правопорядка

cisco

# Когда будут известны критерии?

- Проект Постановления Правительства «Об утверждении показателей критериев категорирования элементов критической информационной инфраструктуры, значений таких показателей, а также порядка категорирования объектов критической информационной инфраструктуры»
- Принятие в течение 6 месяцев после определения ФОИВ, уполномоченного в области безопасности КИИ

cisco

# Кто регулятор?

| ФОИВ по безопасности КИИ | ФОИВ по ГосСОПКЕ | Минкомсвязи | Правительство |
|---|---|---|---|
| • Правила ведения реестра<br>• Проверка правильности категорирования<br>• Требования по безопасности для каждой категории значимых объектов<br>• Госконтроль | • Оценка состояния защищенности<br>• Порядок реагирования на компьютерные инциденты<br>• Порядок ликвидации последствий компьютерных атак<br>• Порядок обмена информацией об инцидентах<br>• Устанавливает на объектах КИИ и сетях электросвязи элементы ГосСОПКИ<br>• Требования к ГосСОПКЕ | • Требования по безопасности для объектов связи и ИТС<br>• Порядок и техусловия установки элементов ГосСОПКИ на сетях электросвязи | • Показатели критериев категорирования<br>• Порядок категорирования<br>• Порядок госконтроля значимых объектов<br>• Порядок подготовки и использования сетей электросвязи для значимых объектов |

# Национальный координационный центр по компьютерным инцидентам


Обмен информацией о компьютерных инцидентах

# Законопроект

## Январь 2016

Принятие в первом чтении

Принятие во втором чтении запланировано на весну 2017

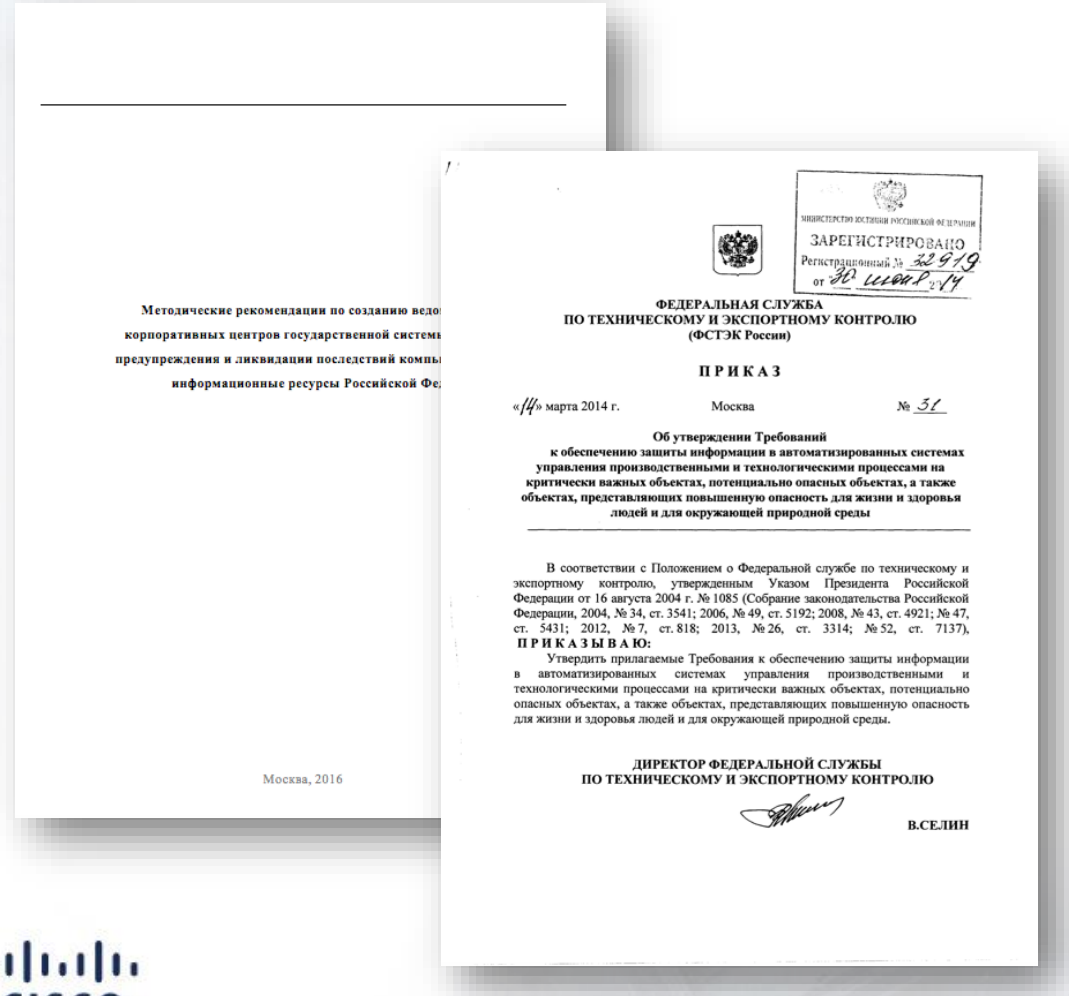
# Какие требования по защите?

- Предотвращение неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения информации на объекте КИИ
- Недопущение воздействия на тех.средства обработки информации, в результате которого может быть нарушено или прекращено функционирование объекта КИИ
- Обнаружение и предупреждение компьютерных атак
- Восстановление функционирования объекта КИИ, в том числе и за счет создания и хранения резервных копий информации
- Непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ
- Сбор, анализ и хранение сведений о проведенных атаках

cisco

# Иерархия требований по безопасности

# Какие документы уже есть?



Методические рекомендации по созданию ведо
корпоративных центров государственной системы
предупреждения и ликвидации последствий компью
информационные ресурсы Российской Фе

Москва, 2016

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 32919
от 30 июня 2014

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

ПРИКАЗ

«14» марта 2014 г. Москва № 31

Об утверждении Требований
к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды

В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818; 2013, № 26, ст. 3314; № 52, ст. 7137),

ПРИКАЗЫВАЮ:

Утвердить прилагаемые Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

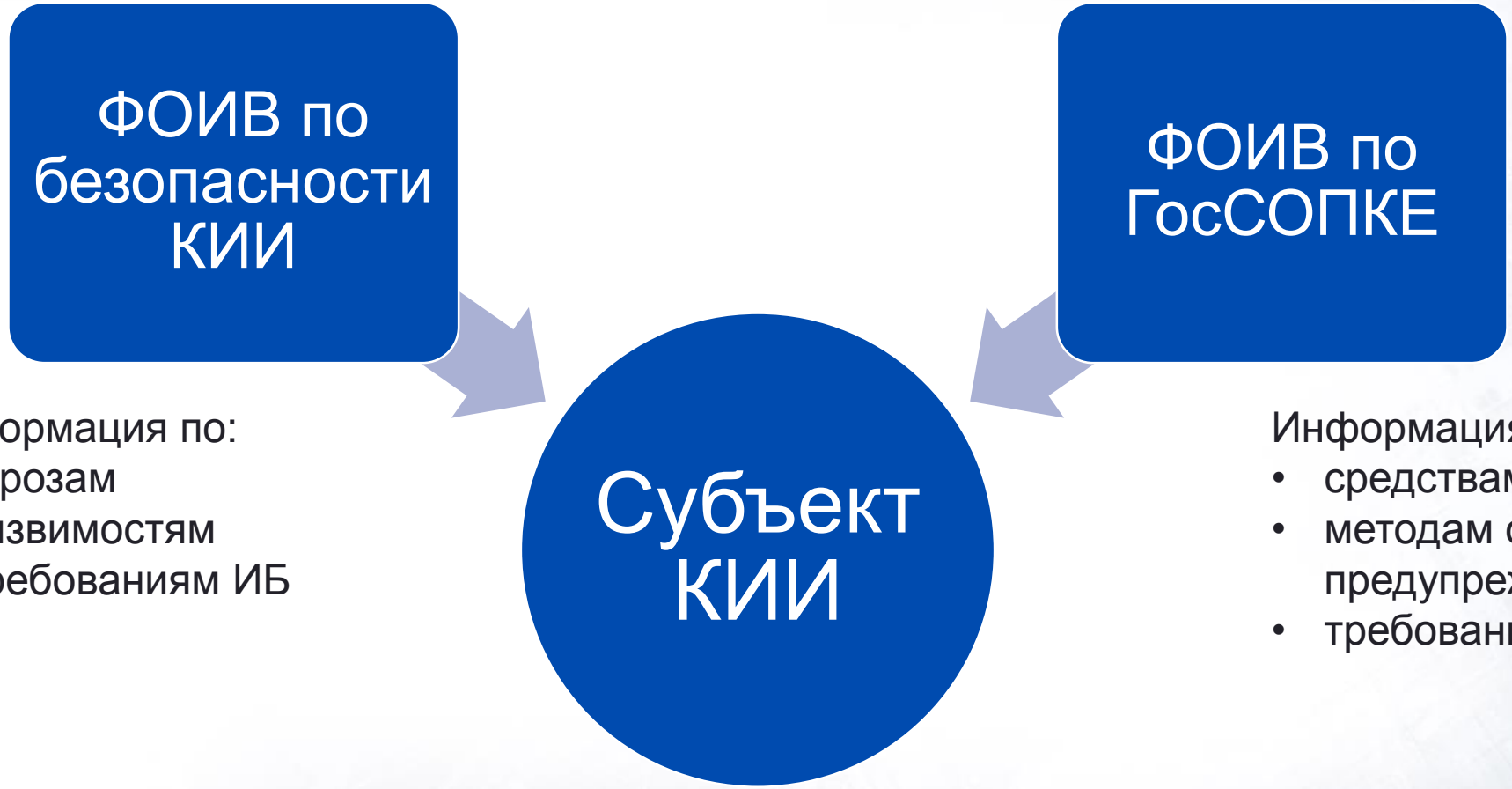
В.СЕЛИН

# Разработаны

- Документы ФСТЭК по КСИИ
- Основы госполитики в области обеспечения безопасности АСУ ТП КВО
- Указ Президента №31с
- ПП-861 по уведомлению об инцидентах на объектах ТЭК
- Методические рекомендации по созданию центров ГосСОПКИ
- Приказ ФСТЭК №31
- РД на промышленные МСЭ

cisco

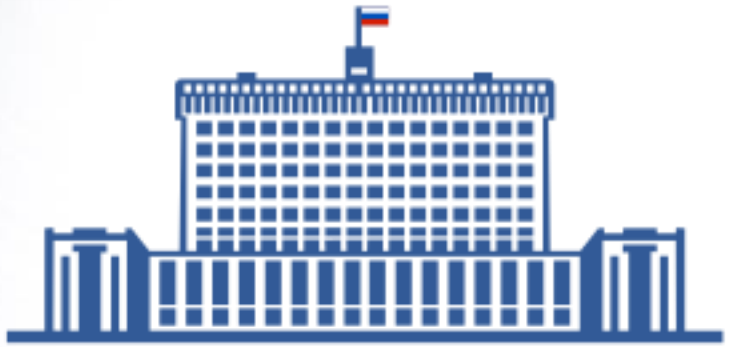
# Что субъекты КИИ могут ждать от регуляторов?




Информация по:
- угрозам
- уязвимостям
- требованиям ИБ

Информация по:
- средствам и способам атак
- методам обнаружения и предупреждения
- требованиям к ГосСОПКЕ

# Какие документы планируется принять?



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

- Постановления Правительства «Об утверждении показателей критериев категорирования элементов КИИ, значений таких показателей, а также порядка категорирования объектов КИИ»
- Постановления Правительства «Об утверждении порядка осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ»
- Постановление Правительства «Об утверждении порядка подготовки и использования ресурсов единой сети связи электросвязи для обеспечения функционирования значимых объектов КИИ»

cisco

# Какие документы планируется принять?


- Поправки в закон о связи
- Приказ Минкомсвязи «Об утверждении требований по обеспечению безопасности значимых объектов КИИ»
- Приказ Минкомсвязи «Об утверждении порядка и технических условий установки и эксплуатации для операторов связи устанавливаемых в сетях электросвязи технических средств, предназначенных для поиска признаков компьютерных атак»

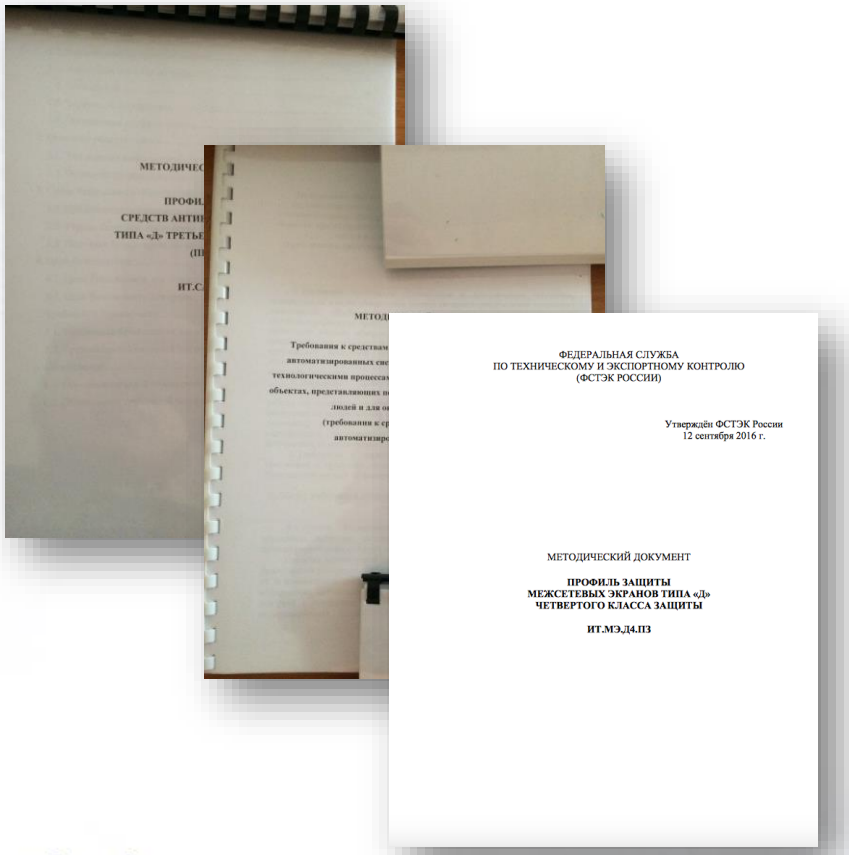
cisco

# Какие документы планируется принять?

- Приказ уполномоченного ФОИВ об утверждении требований по обеспечению безопасности значимых объектов КИИ
- Приказ уполномоченного ФОИВ об утверждении формы предоставления сведений о проведенном категорировании
- Приказ уполномоченного ФОИВ об утверждении формы акта по результатам проведенной проверки в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ
- Приказ уполномоченного ФОИВ об утверждении формы реестра объектов КИИ и правил его ведения

cisco

# Требования ФСТЭК по сертификации промышленных СрЗИ




## Долгосрочная перспектива (2019+)

Предполагается установление требований по оценке соответствия средств защиты информации, используемых для защиты АСУ ТП и, возможно, для объектов критической информационной инфраструктуры

cisco

# Какие документы планируется принять?


- Методика обнаружения компьютерных атак на информационные системы и информационно-телекоммуникационные сети государственных органов и по согласованию с их владельцами - на иные информационные системы и информационно-телекоммуникационные сети
- Порядок обмена информацией между федеральными органами исполнительной власти о компьютерных инцидентах, связанных с функционированием информационных ресурсов Российской Федерации
- Методические рекомендации по организации защиты критической информационной инфраструктуры Российской Федерации от компьютерных атак

cisco

# Какие документы планируется принять?


- Порядок обмена информацией между федеральными органами исполнительной власти и уполномоченными органами иностранных государств (международными организациями) о компьютерных инцидентах, связанных с функционированием информационных ресурсов
- Порядок осуществления деятельности субъектов ГосСОПКИ в области обнаружения, предупреждения и ликвидации последствий компьютерных атак
- Порядок и периодичность проведения мероприятий по оценке степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак

cisco

# Спасибо!

alukatsk@cisco.com