КРОК

АКТУАЛЬНЫЕ ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА ПО БЕЗОПАСНОСТИ КИИ И БЛИЖАЙШИЕ ПЛАНЫ РЕГУЛЯТОРОВ

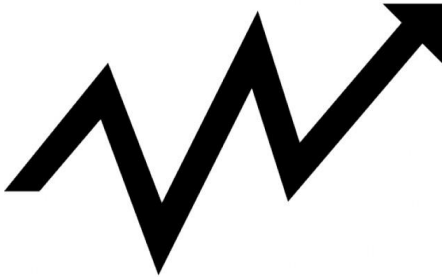
Павел Луцик
Руководитель проектов по информационной безопасности

Москва, 19 сентября 2017

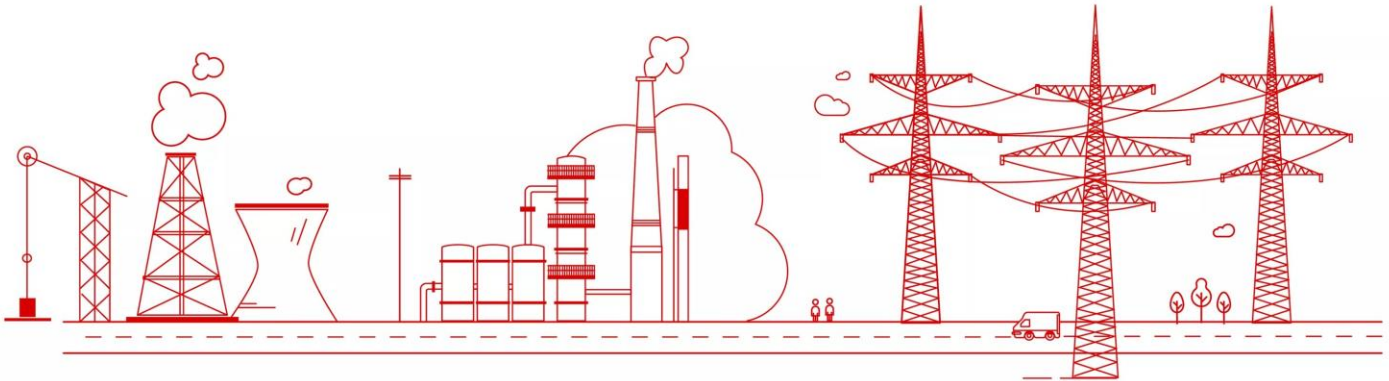
РАЗВИТИЕ ЗАКОНОДАТЕЛЬСТВА О БЕЗОПАСНОСТИ КИИ

КРОК

- 2012 – законопроект ФСТЭК, не внесен в Госдуму
- 2013 – законопроект ФСБ, не внесен в Госдуму
- 06.12.2016 – законопроект ФСБ, внесен в Госдуму
- 26.07.2017 – принятие пакета из трех ФЗ по безопасности КИИ
- 2017-2018 – принятие подзаконных актов



187-ФЗ от 26.07.2017 «О безопасности КИИ РФ»



КЛЮЧЕВЫЕ ПОНЯТИЯ

- **КИИ**
  - ✓ Объекты КИИ и сети электросвязи
- **Объекты КИИ**
  - ✓ Информационные системы субъектов КИИ
  - ✓ Сети субъектов КИИ
  - ✓ АСУ субъектов КИИ

- **Субъекты КИИ**
  - ✓ Владельцы объекта КИИ
  - ✓ Лица или организации, обеспечивающие взаимодействие объектов КИИ
  - ✓ Лицо, эксплуатирующее объект КИИ (оператор)

СФЕРЫ ОБЪЕКТОВ КИИ

- **Финансовая сфера**
- **Здравоохранение**
- **Транспорт**
- **Энергетика**
- **Наука**
- **Связь**
- **ТЭК**

- **Область атомной энергии**
- **Промышленность**
  - ✓ Оборонная
  - ✓ Ракетно-космическая
  - ✓ Горнодобывающая
  - ✓ Металлургическая
  - ✓ Химическая

РЕГУЛЯТОРЫ

КРОК

ФОИВ по безопасности КИИ (БКИИ)

- Правила ведения реестра
- Проверка категорирования
  Требования по безопасности
- Государственный контроль

Минкомсвязи

- Требования по безопасности для операторов связи
- Порядок и условия установки ГосСОПКА на сетях связи

ФОИВ по ГосСОПКА

- Оценка состояния защищенности
- Порядок реагирования на инциденты
- Порядок ликвидации последствий атак
- Порядок взаимодействия с ГосСОПКА
- Требования к ГосСОПКА

Правительство

- Показатели критериев категорирования
- Порядок категорирования
- Порядок госконтроля
- Порядок подготовки и использования сетей связи для значимых объектов

ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО 187-ФЗ

- **Категорирование объектов КИИ**
- **Обеспечение ИБ**
- **Присоединение к ГосСОПКА**

КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ КИИ

КРОК

Критерии

- Социальной значимости
- Политической значимости
- Экономической значимости
- Экологической значимости
- Значимости для обеспечения обороноспособности

Категории значимости

- Первая
- Вторая
- Третья

Типы объектов КИИ

- Значимые
- Не значимые

ОБЕСПЕЧЕНИЕ ИБ НА ЗНАЧИМЫХ ОБЪЕКТАХ КИИ

КРОК

№	Требования по защите информации	Возможные меры защиты
1	Предотвращение НСД, уничтожения, блокирования и т.д. информации	**СЗИ от НСД**
2	Недопущение воздействия на ТСОИ на объекте КИИ	**Меры физ.безопасности**
3	Обнаружение и предупреждение компьютерных атак	**СОА (IDS/IPS)**
4	Восстановление функционирования объекта КИИ, в том числе за счет резервного копирования	**Backup**
5	Сбор, анализ и хранение сведений о проведенных атаках	**SIEM**

ПРИСОЕДИНЕНИЕ К ГОССОПКА

- Установка средств обнаружения вторжений атак (СОА)
- Информирование об инцидентах (ФСБ, ЦБ)
- Выполнение правил реагирования на инциденты
- Беспрепятственный доступ сотрудников ФСБ на объекты КИИ

193-ФЗ ОТ 26.07.2017 «О ВНЕСЕНИИ ИЗМЕНЕНИЙ В …»

- **в ФЗ «О государственной тайне»**
  - ✓ Сведения о мерах по защите значимых объектов КИИ
  - ✓ Сведения об оценке степени защищенности объектов КИИ
- **в ФЗ «О связи»**
  - ✓ Обязанность оператора связи обеспечить условия эксплуатации средств ГосСОПКА
- **в ФЗ «О защите прав юридических лиц…»**
  - ✓ не будет применяться при проверках объектов КИИ

194-ФЗ ОТ 26.07.2017 «О ВНЕСЕНИИ ИЗМЕНЕНИЙ В УК И УПК РФ…»

КРОК

№	Новая статья 274.1 в УК РФ (дела по ней рассматривает ФСБ)	Ответственность
1	Создание, распространение, использование ПО либо иной компьютерной информации для неправомерного воздействия на КИИ	До **5 лет**, со штрафом
2	Неправомерный доступ к охраняемой информации в КИИ, повлекший причинение вреда КИИ	До **6 лет**, со штрафом
3	Нарушение правил эксплуатации и правил доступа, повлекшее причинение вреда КИИ	До **6 лет**, с лишением права занимать должность
4	Все предыдущие деяния по сговору или с использованием служебного положения	До **8 лет**, с лишением права занимать должность
5	Все предыдущие деяния, повлекшие тяжкие последствия	До **10 лет**, с лишением права занимать должность

ПЛАНЫ РЕГУЛЯТОРОВ

КРОК

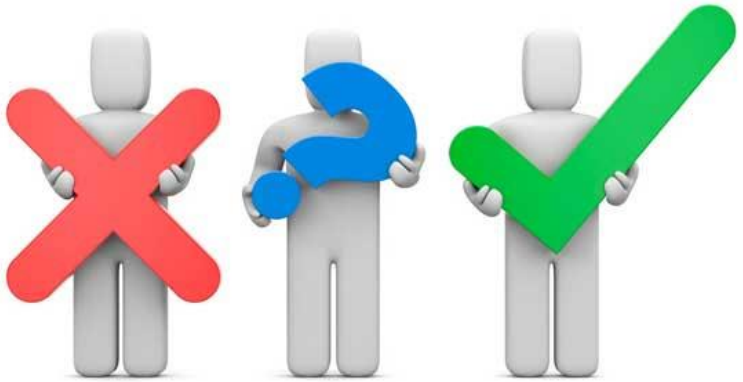
№	Планы	Сроки
1	**- Вступление в силу пакета ФЗ по безопасности КИИ**	**01.01.2018**
2	**- Определение ФОИВов по безопасности КИИ и по ГосСОПКА (Президент)** - Порядок подготовки и использования сети электросвязи для обеспечения функционирования значимых объектов КИИ (Правительство)	**п.1 + 6 мес.**
3	**- Порядок реагирования на инциденты (ФСБ)** **- Порядок установки и эксплуатации средств ГосСОПКА для операторов связи (ФСБ)** - Порядок передачи сведений в ГосСОПКА и получения их из нее (ФСБ) - Требования к техническим средствам ГосСОПКА, условия их эксплуатации (ФСБ) - Положение о национальном координационном центре (ФСБ)	**п.2 + 3 мес.**
4	- **Порядок категорирования объектов КИИ (Правительство)** **- Требования по обеспечению безопасности значимых объектов КИИ (ФОИВ ПО БКИИ)** - Требования по обеспечению безопасности значимых объектов КИИ (Минкомсвязь) - Порядок государственного контроля (Правительство) - Форма предоставления сведений о категорировании (ФОИВ по БКИИ) - Правила ведения реестра объектов КИИ (ФОИВ по БКИИ)	**п.2 + 6 мес.**

ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ И НАДЗОР

КРОК

- **ФОИВ по безопасности КИИ**
- **Плановая проверка**
  - ✓ раз в три года
- **Внеплановая проверка проводится**
  - ✓ по истечению срока предписания
  - ✓ инцидент
  - ✓ поручение Президента, Правительства
  - ✓ требование прокурора

ИТОГО



- Категорирование
- Присоединение к ГосСОПКА
- Реализация требований по ИБ
- Сбор, хранение информации об атаках, выстраивание процесса реагирования на них
- Организация «Первого» отдела под Гостайну

КРОК

СПАСИБО ЗА ВНИМАНИЕ!

Павел Луцик
Руководитель проектов по ИБ

111033, Москва, ул. Волочаевская, д.5, к.1
Т: (495) 974 2274 | Ф: (495) 974 2277
E-mail: PLutsik@croc.ru
croc.ru