ITSF

XIII ЦИФРОВОЙ ФОРУМ

Практика категорирования объектов КИИ

Петров Илья

Руководитель группы продвижения решений

ICL Системные технологии

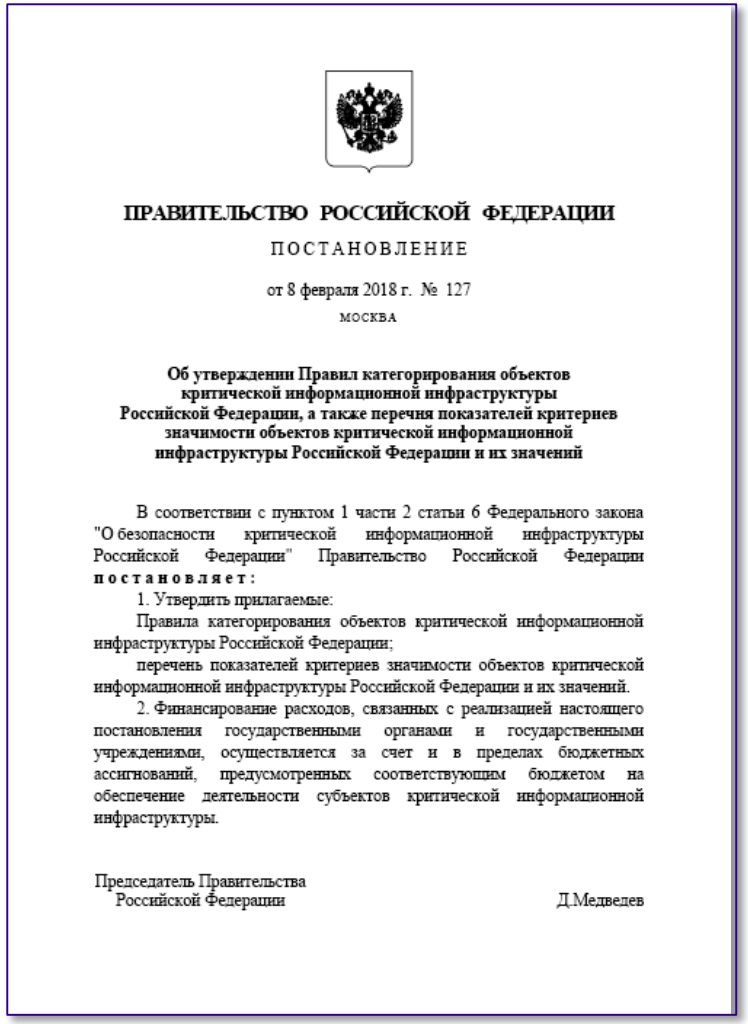
Состав мероприятий

Категорирование объектов КИИ	Создание системы обеспечения информационной безопасности (СОИБ) значимых объектов КИИ
Проектирование СОИБ	Создание системы управления информационной безопасностью (СУИБ) и подключение к ГосСОПКА
2019 - 2020	2020-2022

Привести в соответствие с требованиями 187-ФЗ до 2022 года

Перечень работ

- Создать комиссию по категорированию
- Выявить критичные процессы
- Выявить перечень объектов КИИ, обеспечивающих функционирование критичных процессов
- Описать состав технических и программных средств объектов КИИ, указать подключение к сетям
- Провести моделирование угроз для каждого объекта КИИ
- Провести оценку соответствия критериям значимости
- **Подготовить акты категорирования по объектам КИИ и отправить сведения во ФСТЭК России по их форме (Приказ № 236 от 22.12.2017)**



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 8 февраля 2018 г. № 127

МОСКВА

Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений

В соответствии с пунктом 1 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые:

Правила категорирования объектов критической информационной инфраструктуры Российской Федерации;

перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений.

2. Финансирование расходов, связанных с реализацией настоящего постановления государственными органами и государственными учреждениями, осуществляется за счет и в пределах бюджетных ассигнований, предусмотренных соответствующим бюджетом на обеспечение деятельности субъектов критической информационной инфраструктуры.

Председатель Правительства
Российской Федерации Д.Медведев

Формирование комиссии по категорированию

- Собрать комиссию на базе ПДТК
- Включить ответственных за технологические процессы

Процессы и их критичность

- Разделить на производственные и вспомогательные
- Провести декомпозицию
- Оценивать критичность подпроцессов по критериям ПП №127

Единообразие процессов, формирование единого перечня процессов из Головной организации

Формирование перечня объектов КИИ

- Установить границы объекта КИИ
- Типизировать объекты КИИ (назначение, функционально-технические характеристики, масштаб)
- Обеспечить единообразие на уровне:
  - Наименований объектов КИИ
  - Привязка к бизнес\технологическому процессу

Выявление актуальных угроз

- Определить векторы потенциальных атак и возможных инцидентов
- СрЗИ не учитываются при оценке актуальности угрозы
- Исходные данные - архитектурные особенности, используемые технологии, источники угрозы (БДУ ФСТЭК)

Оценка по критериям значимости

- Возможен ли останов объекта или авария вследствие компьютерной атаки/инцидента?
- Возможен ли ущерб от останова/аварии?
- Каков размер ущерба?
- Какие обоснования/свидетельства нужно собрать?

Возможен ли останов объекта?

Вопрос к отв. за эксплуатацию АСУ ТП, метрологам:

- Если злоумышленник получил административный доступ - сможет ли он остановить объект, спровоцировать аварию?
- Есть ли дублирующие системы (**не цифровые**):
  - ручное управление/ ручное измерение параметров тех.процесса
  - автоматические защитные устройства (отсекатели, клапаны и т.п.);
  - независимая от системы ПАЗ
  - независимое от системы резервное управление

Возможен ли ущерб?

Вопрос	Кому
Возможно ли возникновение человеческих жертв вследствие аварии?	Эксплуатация объекта КИИ, служба метрологии
Может ли вследствие нарушение работы объекта произойти вредное воздействие на окружающую среду?	Эксплуатация объекта КИИ, экологическая служба
Может ли произойти прекращение передачи потребителям тепловой энергии?	Эксплуатация объекта КИИ, служба метрологии

Каков размер ущерба?

Вопрос	Кому
Максимальное количество человеческих жертв вследствие аварии?	Эксплуатация объекта КИИ, служба метрологии
Каково максимальное время восстановления передачи потребителям тепловой энергии?	Эксплуатация объекта КИИ, служба метрологии
Каково максимальное время восстановления работоспособности и время запуска объекта?	Эксплуатация объекта КИИ, служба метрологии
Какова сумма недополученной прибыли за выработку электроэнергии вследствие простоя объекта?	Эксплуатация объекта КИИ, служба сбыта

Пример расчёта экономического ущерба

Совокупная недополученная прибыль на время простоя

+

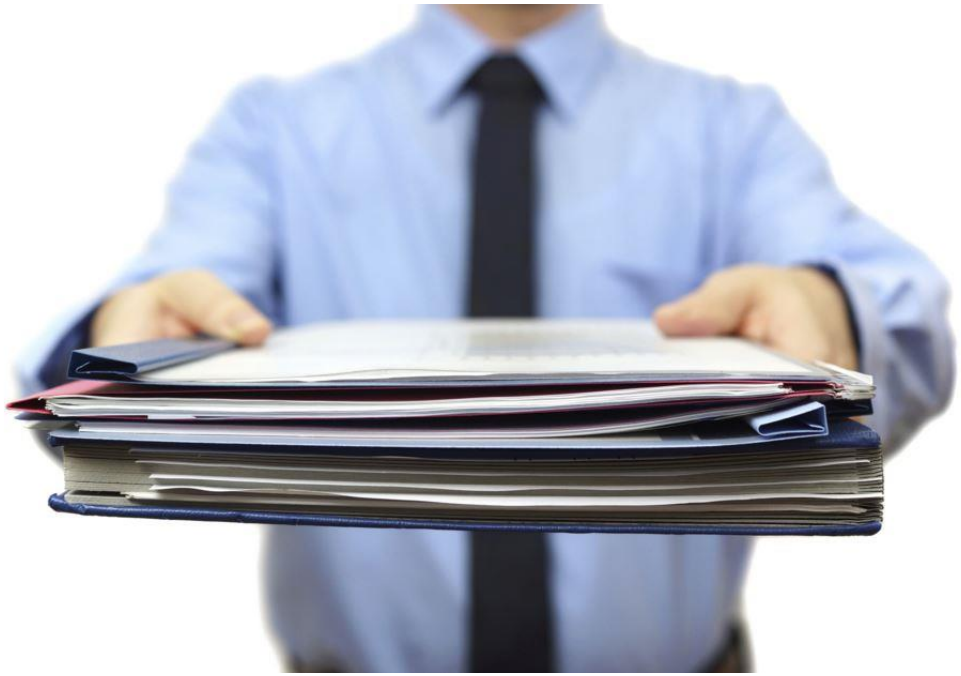
Штрафы

+

Стоимость восстановления объекта

Свидетельства и обоснования

- Декларация пром. безопасности ОПО
- Паспорт безопасности объекта ТЭК
- Пояснительные записки, протоколы и т.д.



Если Вы всё сделали правильно…

Отдел обеспечения безопасности критической информационной инфраструктуры ФСТЭК России <otd25@fstec.ru>

Ответ на обращение

Кому Павлюкевич Дмитрий Иванович

Мы удалили дополнительные разрывы строк в сообщении.

Дмитрий Иванович!

Сведения о результатах присвоения объектам критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения им таких категорий, представленные ОАО «Сетевая Компания», в ФСТЭК России рассмотрены.

В соответствии с частью 7 статьи 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» уведомляем о внесении указанных сведений в Реестр значимых объектов критической информационной инфраструктуры Российской Федерации:

Сведения об отсутствии необходимости присвоения объектам критической информационной инфраструктуры Российской Федерации категорий значимости проверены и направлены в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

--

С уважением,
Отдел обеспечения безопасности критической информационной инфраструктуры ФСТЭК России
(5 отдел 2 управления ФСТЭК России)

Тел.: (499) 246-11-89
Эл. почта: otd25@fstec.ru
Вэб-сайт: www.fstec.ru

Средства автоматизации

- Обеспечение единообразия, организация совместной работы
- Сбор инвентаризационных данных
- Автоматизация анализа угроз
- Оценка по критериям, формирование требуемых отчётных документов
- Сбор и хранение в единой точке обоснований и свидетельств

Оптимизация затрат и сроков категорирования объектов КИИ

ITSF

Итоги

- Единообразие состава и наименований
- Типизация объектов КИИ
- Правильные вопросы
- Обоснования и свидетельства
- Использование средств автоматизации

СПАСИБО ЗА ВНИМАНИЕ!

Компания ICL Системные технологии

420029, Казань, Сибирский тракт, 34
Телефон: +7(843) 279-58-23
Факс: +7(843) 279-49-05
Электронная почта: info@icl.kazan.ru
Веб-сайт: www.icl.ru