

Юридические и практические аспекты защиты информации в сфере транспортной безопасности

1

Определить принадлежность организации к субъектам критической инфраструктуры/ ГИС/ ИСПДн

2

Создать комиссию и провести категорирование объектов КИИ / классификацию ГИС и определение УЗ для ИСПДн

3

Создать комплексную систему безопасности

4

Организовать взаимодействие с Национальным координационным центром по компьютерным инцидентам (НККИ) ФСБ России

5

Провести аттестацию системы



Законодательство

КИИ

ФЗ-187
«О безопасности КИИ
Российской
Федерации»

ПП- № 127
«Правила
категорирования
объектов КИИ...»

Приказ ФСТЭК России
№ 235
«Требования к
созданию СБ КИИ РФ»

Приказ ФСТЭК России
№ 239
«Требования по обесп.
безопасности КИИ
РФ»

ГИС

ФЗ-149
«Об информации,
ИТ и о ЗИ»

ПП- № 676
«Требования к порядку
создания, развития,
ввода ГИС...»

Приказ ФСТЭК России
№ 17
«ЗИ, не составляющей
ГТ, содержащейся в
ГИС»

ИСПДн

ФЗ -152
«О персональных
данных»

ПП -1119
«Требования по
защите ПДн»

Приказ ФСТЭК России
№ 21
«О защите ПДн»

Приказ ФСБ России
№ 378
«Защита ПДн с
использованием
СКЗИ»



Принадлежность организации к субъектам КИИ

1

Здравоохранение

Наука

Транспорт

Связь

Банковская сфера

Финансовый рынок

ТЭК

Энергетика

Атомная энергия

Оборонная
промышленность

Космическая
промышленность

Горнодобывающ
ая
промышленность

Металлургия

Химическая
промышленность





Создание комиссии и категорирование



Создание комиссии

Определение состава комиссии по категорированию объектов КИИ
Издание приказа о создании комиссии



Определение критических процессов

Выявление критических процессов в организации
(управленческий, технологический, производственный и т.п.)



Определение перечня объектов КИИ

Разработка перечня объектов, подлежащих категорированию
Согласование перечня с отраслевым Регулятором
Отправка перечня в ФСТЭК России



Определение угроз безопасности

Определение угроз безопасности
Определение перечня уязвимостей

Категорирование и классификация

Определение категории значимости, класса защищенности и уровня защищенности



Создание комплексной системы безопасности

3



Определение требований

- Определение требований в соответствии с категорией значимого и класса системы
- Разработка ТЗ на систему защиты



Разработка мер защиты

- Анализ угроз безопасности
- Проектирование системы защиты
- Разработка эксплуатационной документации



Внедрение мер защиты

- Установка и настройка средств защиты
- Разработка ОРД
- Испытания системы защиты
- Анализ уязвимостей



Эксплуатация

- Обеспечение безопасности системы в ходе ее эксплуатации
- Реагирование на компьютерные инциденты
- Обучение персонала





Типовой перечень основных подсистем СИБ



Взаимодействие с НКЦКИ (ФСБ России)

Разработка Регламента

- порядок информирования
- перечень информации

Подключение к технической инфраструктуре НКЦКИ

www.gov-cert.ru



Создание ведомственного сегмента ГосСОПКА

- Персонал
- Технические средства
- Документация

Информационный обмен

- Информация об атаках
- Информация о возможных атаках
- Экспертиза критических событий



Аттестация проводится в случае если

Значимый объект КИИ является государственной информационной системой (ГИС)

Значимый объект КИИ обрабатывает гостайну

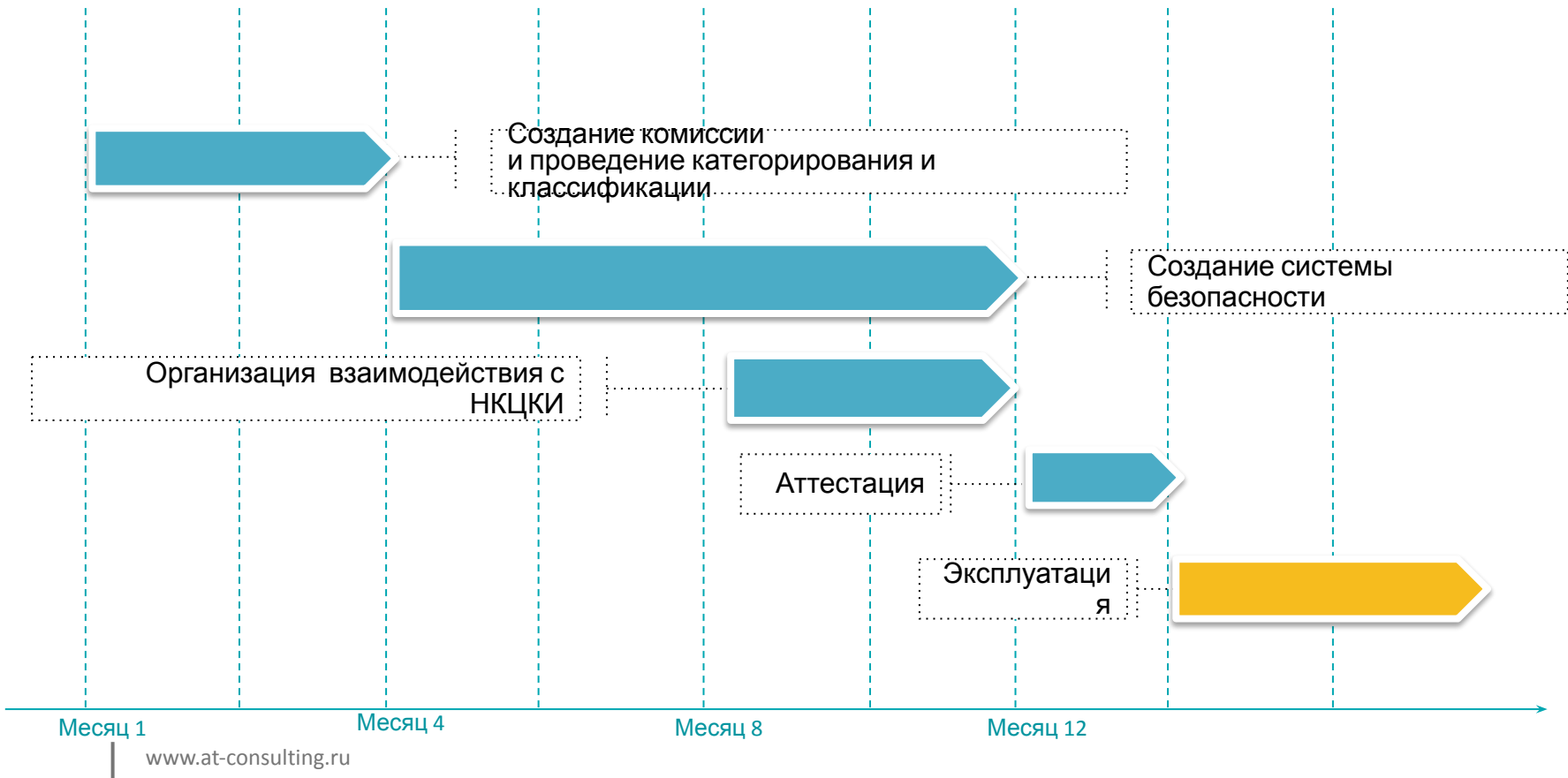
В организации принято решение по проведению аттестации

в остальных случаях

Проводится подтверждение соответствия объекта КИИ требованиям законодательства в ходе приемочных испытаний



Общий мастер-план





AT Consulting

Спасибо за внимание!

127015, Россия, Москва,
ул. Большая Новодмитровская, д. 14, стр.
2
Офисный центр «Новодмитровский»

Тел.: +7 (495) 748-05-75
Факс: +7 (495) 748-01-25
e-mail: clients@at-consulting.ru

www.at-consulting.ru