Эшелон
комплексная безопасность

# Проблемы и практика категорирования КИИ. Взгляд со стороны эксперта

Мотылев Игорь
Руководитель группы аудита и консалтинга

# Кто отвечает за защиту значимых объектов КИИ?

Обычно «вешают» проблему на специалиста по ИБ, реже на специалиста по Compliance, которые…

- ✓ имеют много других проектов и обязанностей
- ✓ часто имеют недостаток в квалифицированных помощниках
- ✓ не всегда имеют должную глубокую подготовку по вопросам КИИ
- ✓ воспринимают тематику КИИ скорей, как разовый проект, а не постоянный процесс
- ✓ не имеют рычагов воздействия на ситуацию и другие подразделения Компании
- ✓ не имеет официальной методологии как приступить к фазам работ по КИИ, как и каким образом что-то делать по КИИ

Категорирование осуществляет постоянно действующая Комиссия по категорированию

# Основные рекомендации

- читайте «придирчиво» нормативные требования
- смотрите не только нормативные требования *очевидно* связанные с КИИ, но и иные (не только № 187-ФЗ). Смотрите на задачу шире
- не все нужно делать «с нуля» - много у вас уже сделано (ГИС, АСУТП)
- документируйте и храните результаты работы
- Выделяйте (привлекайте) в работу специалистов разного профиля
- извлекайте выгоду из проделанной работы

# I. КИИ – это не разовый Проект

Мы субъект КИИ ? → Формировать комиссию по КИИ → Сформировать перечень ОКИИ → Проведение Категорирования

# II. Опыт категорирования

## Мы субъект КИИ ?

Читаем определение (8 Статьи 2 из 187- ФЗ) до конца + 127 ПП:

- ...на праве собственности, аренды или на ином законном основании…
- …функционирующие в одной из 13 сфер…
- …. или обеспечивают взаимодействие указанных систем или сетей
- Нет явного упоминания подведомственности, как критерия

**Право собственности - что использовать:**

- ✓ сведения из федеральной ГИС учета ИС, создаваемых и приобретаемых за счет средств бюджета (федерального или государственных внебюджетных фондов и аналогичных ИС учета субъектов РФ;
- ✓ договор на разработку и внедрение ИС, ИТКС, АСУ
- ✓ проектная документация на ИС, ИТКС, АСУ
- ✓ локальные нормативные акты юрлица, вводящие Положение о порядке использования или о вводе в эксплуатацию ИС, ИТКС, АСУ
- ✓ данные бухгалтерского учета по разделу «основные средства», «нематериальные активы»

# II. Опыт категорирования

## Мы субъект КИИ ?

**Сферы деятельности* и подведомственность - что использовать:**

- ✓ Учредительные документы (Закон о создании госкорпорации, положение/приказ о создании ФГУП, ГУП, МУП, **устав организации**, учредительный договор)
- ✓ Коды ОКВЭД
- ✓ Заявление о госрегистрации
- ✓ Выписка из ЕГРЮЛ
- ✓ Декларацию промышленной безопасности
- ✓ Имеющиеся лицензии на виды деятельности (ФЗ-99 и др.)

«Подведомственность» требуется для предварительного согласования перечня объектов КИИ

**Взаимодействие указанных <u>систем</u> или <u>сетей</u> - что использовать :**

- ✓ договоры на оказание услуг сторонним организациям
- ✓ регламенты взаимодействия с другими ИС, ИТКС, АСУ

При необходимости отправить запрос взаимодействующим юрлицам о его принадлежности к субъектам

* осуществляется по кодам видов деятельности в соотв. с Общероссийским классификатором ОК 029-2014

# II. Опыт категорирования

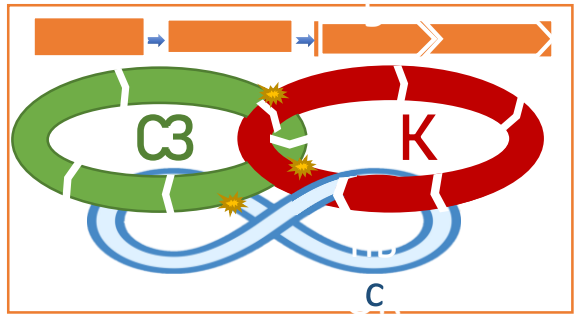
Формировать комиссию по КИИ

## Категорирование осуществляет постоянно действующая Комиссия по категорированию

- ✓ Комиссию по категорированию возглавляет руководитель субъекта (или уполномоченное им лицо)
- ✓ Настоятельно рекомендуется включать в нее специалистов :
  - по **видам деятельности (бизнес процессам)**, бизнес аналитик
  - по ИБ, ИТ, гражданской обороне и защите от чрезвычайных ситуаций, Гостайны (при необходимости),
  - **финансово-экономического подразделения**
  - **юрист**
- ✓ В состав комиссии по категорированию могут включаться представители государственных органов

Комиссия по категорированию работает постоянно, в частности:

- ✓ перекатегорирование ОКИИ (регулярно или при изменениях)
- ✓ Появляются новые / изменяются ОКИИ (ИС, АСУТП, ИТКС)
- ✓ Изменяется законодательство РФ



# II. Опыт категорирования

Сформировать перечень ОКИИ *

**перечень объектов** критической информационной инфраструктуры, подлежащих категорированию

Перечень бизнес процессов → Анализ и оценка бизнес процессов → Выделение критических процессов → Анализ и оценка ОКИИ → Перечень ОКИИ

Согласование списка

**перечень объектов** критической информационной инфраструктуры, подлежащих категорированию

Категорирование ОКИИ

ПереКатегорирование ОКИИ



* Что такое *ОКИИ* = ИС, ИТКС, АСУ субъектов КИИ

# II. Опыт категорирования

Сформировать перечень ОКИИ *



Перечень бизнес процессов

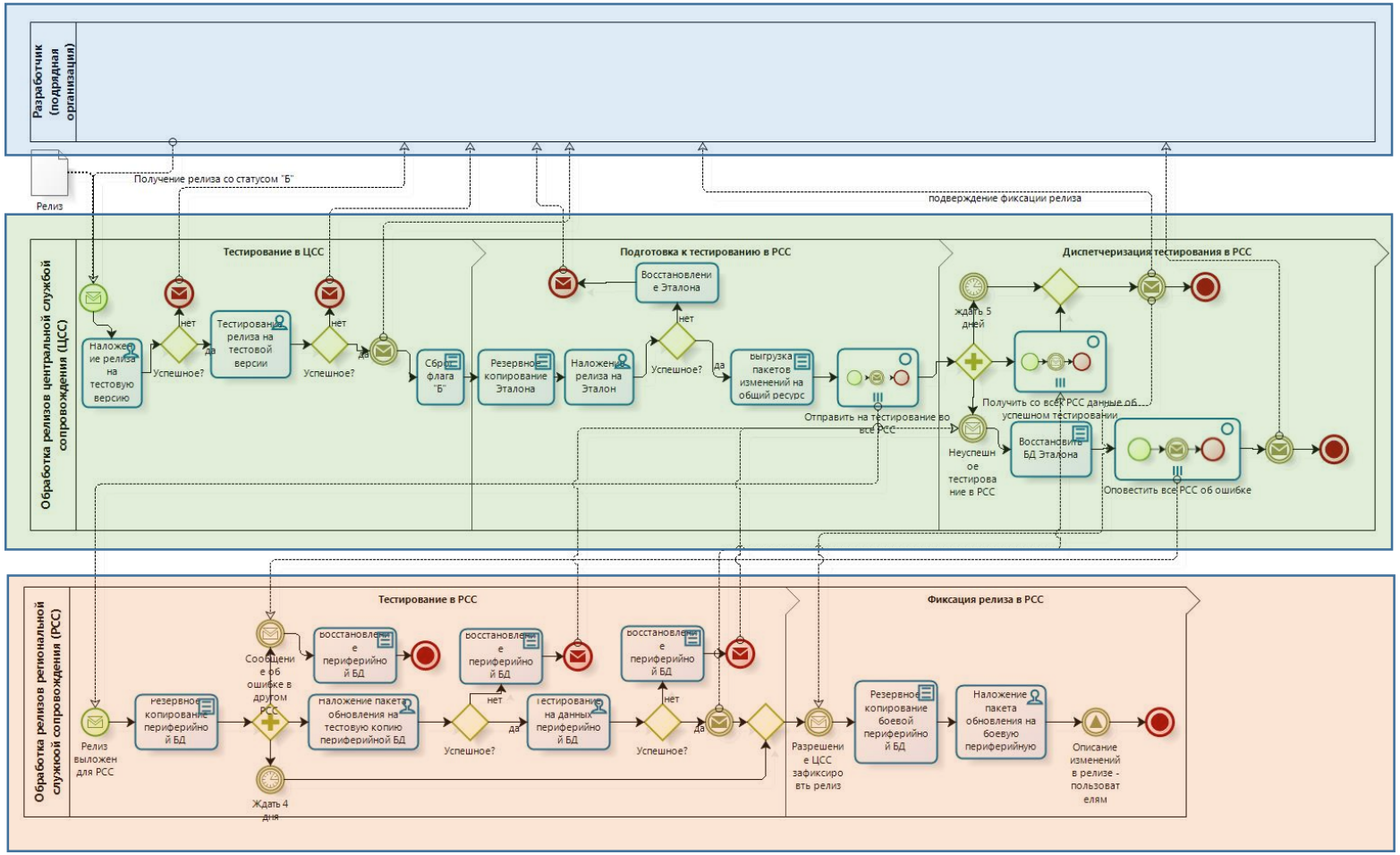
## Где взять перечень бизнес процессов?

**Если были описаны процессы…**

- ✓ Реестр бизнес процессов
- ✓ Регламенты выполнения функций
- ✓ Технологические карты
- ✓ Диаграммы потоков данных

## Крайне полезно для целей

- ✓ Понимать ЧТО делает организация
- ✓ Понимать КТО и КАК это делает
- ✓ Определять проблемы (в т.ч. ИБ)
- ✓ Определять ИС и данные
- ✓ Внятно вносить изменения



# II. Опыт категорирования

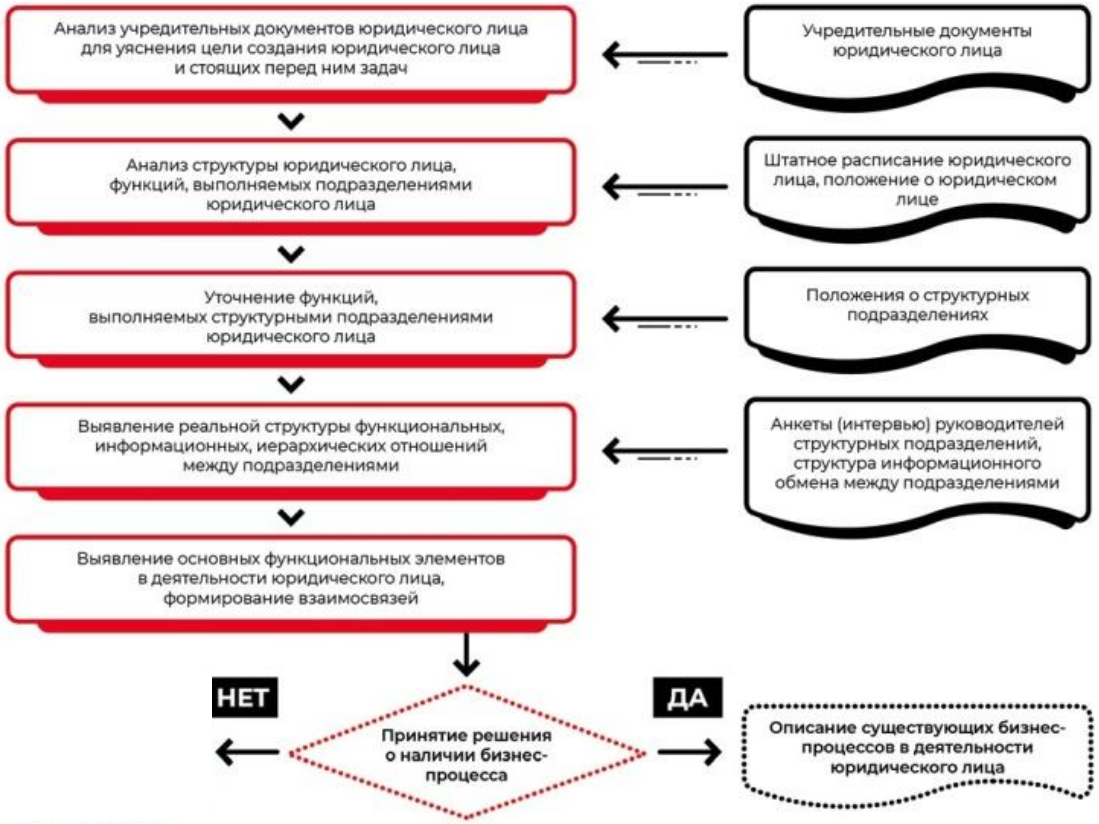
Сформировать перечень ОКИИ *

Перечень бизнес процессов

## Где взять перечень бизнес процессов?

**Если не были описаны процессы …**

- Упрощенное выявления бизнес-процессов
- Есть референтные (типовые) модели бизнес процессов:
  - ✓ Эталонная модель ИСО/МЭК ТО 15504
  - ✓ Референтная модель BIAN
  - ✓ eTOM (The enhanced Telecom Operations Map)
  - ✓ 8-процессная модель "BKG Profit Technology”
  - ✓ Классификатор типовых процессов APQC
  - ✓ ITSM - IT Service Management (управление IT-обслуживанием)
  - ✓ Стандарты качества банковской деятельности (АРБ)
  - ✓ Типовая модель системы качества образовательного учреждения




Вихорев Сергей «Эссе о бизнесе, процессах и категорировании КИИ»

# II. Опыт категорирования

Перечень бизнес процессов → Анализ и оценка бизнес процессов → Сформировать перечень ОКИИ *

Выявить среди процессов: *управленческие*, *технологические*, *производственные*, *финансово-экономические* и *иные* * …. в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ

☑ определение этих *видов* процессов есть в 127 ПП

Провести анализ

☑ возможных действий нарушителей, последствий от компьютерных атак

☑ анализ взаимного влияния процессов

**Проблемы**

☒ методологии нет (в т.ч. нарушения насколько длительное)

☒ очень высокая специфика отрасли

* Есть в ГОСТ Р 9000, ГОСТ 14.004-83, ГОСТ 3.1109-82, Словарь терминов МинФин России

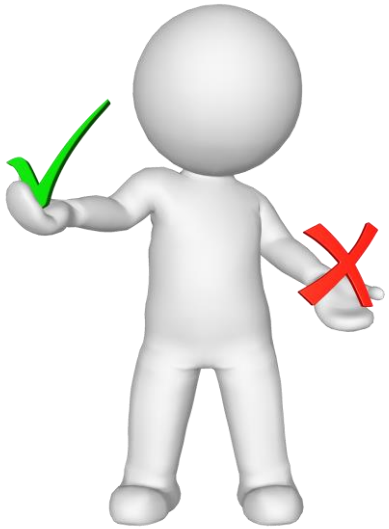
# II. Опыт категорирования

Анализ и оценка бизнес процессов → Выделение критических процессов → Сформировать перечень ОКИИ *

- ✓ Определить влияния и потенциальные последствия по «направлениям»
  - социальной;
  - политической;
  - экономической;
  - экологической;
  - обеспечения обороны страны, безопасности государства и правопорядка

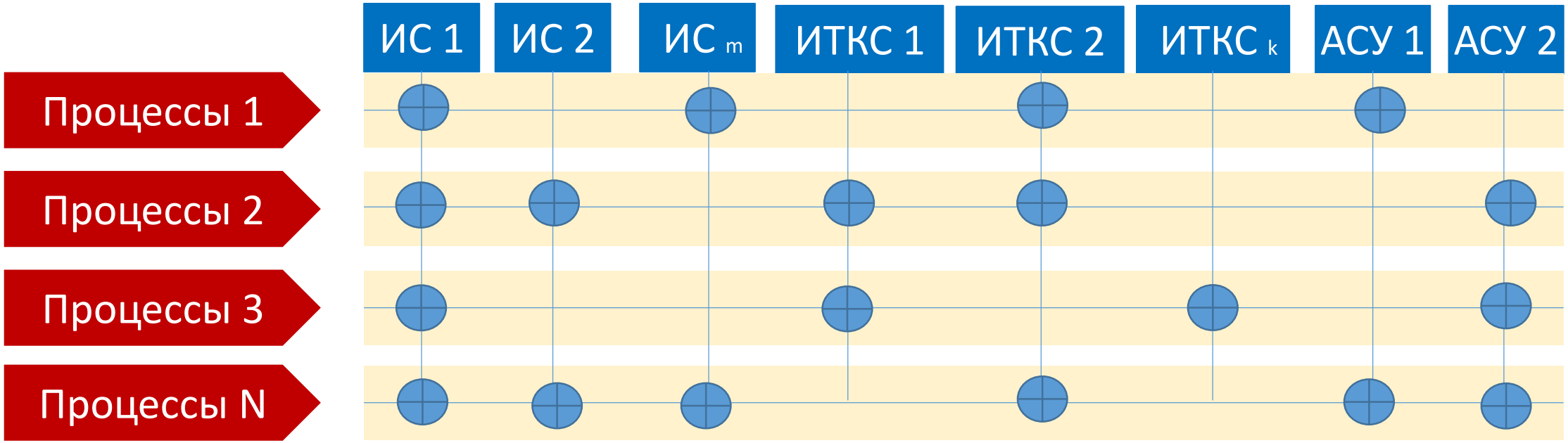
127-ПП (Приложение)

- ✓ **высокоуровневая** оценка («есть или нет»)
- ✓ очень высокая специфика отрасли



# II. Опыт категорирования

- Выявить какие ИС, ИТКС, АСУ ТП поддерживают бизнес процессы (все они объекты КИИ)
- Какие из них поддерживают **Критические** бизнес- процессы, обрабатывают информацию и/или осуществляют управление, контроль или мониторинг



# II. Опыт категорирования

Проведение Категорирования



Детально

- по всем показателям .. по всем критериям (Приложение ПП127)
- по всем ОКИИ (не только по «Перечиню ОКИИ» направленных 1-ый раз в ФСТЭК России)

Только после категорирования *некоторые* ОКИИ получат статус «значимых» (ЗОКИ)

**Проблемы**

☒ методологии нет

☒ очень высокая специфика отрасли

Рекомендации

☑ Контролировать появление/изменение бизнес-процессов, ИТ-систем, систем ИБ

☑ Разработать заранее методику Категорирования «..что считать…»

# III. Внедрение и поддержка

Мы субъект КИИ ? → Формировать комиссию по КИИ → Сформировать перечень ОКИИ → Проведение Категорирования

# III. Внедрение и поддержка

**Проблемы**

☒ методологии нет

☒ Нужны сотрудники на постоянную работу (подразделение)

**Рекомендации**

☑ Разработать процессы поддержки и внедрения + приказы

☑ Назначить **Кураторов за блок(и) ОКИИ** – знать «что там происходит»

☑ Контролировать появление/изменение бизнес-процессов, ИТ-систем, систем ИБ

- Категорирование проводится уже при проектировании…. желательно **Куратор**
- При изменение бизнес-процессов, провести анализ – возможно перекатегорирование
- После внедрения ИС/АСУ/ИТКС передать ее на мониторинг

# Основные проблемы

## Предприятия/Компании

- Максимально оттягивают сроки начала Проекта по КИИ
- Не хватает подготовленных специалистов по КИИ
- Слабая вовлеченность представителей *смежных* подразделений в проект КИИ, часто это *второстепенная* задача даже для специалистов ИБ
- Часто это воспринимается как разовый проект, а не постоянный процесс
- Недостаточный уровень зрелости Компаний по направлению «Процессы», «ИТ вовлеченность»
- Сложности финансирования/выделения ресурсов

## Причины

- Не очевидны выгоды от реализации требований по КИИ, но очевидны *последствия*
- Не полная нормативно-методическая база по КИИ (в т.ч. расплывчатость формулировок)
- Нет доступных «типовых» отраслевых решений
- Реальная практика применения норм и требований закона – отсутствует
- Работы по направлению КИИ весьма затратны

# Предложения

- ✓ Разработать отраслевые методики категорирования
- ✓ Разработать методику для Приказу ФСТЭК №239
- ✓ Предложить регламент работы подразделения по КИИ
- ✓ Создать типовые решения по обеспечению безопасности значимых ОКИИ, с применением отечественных программно-аппаратных решений
- ✓ Предоставить льготы компания по работам в области КИИ:
  - ✓ создание региональных/отраслевых центров ГосСОПКА
  - ✓ создание отечественных программно-аппаратных решений КИИ
  - ✓ работы по созданию обеспечению безопасности значимых ОКИИ

# Наш подход к выполнению проектов по КИИ



1. Подготовка
   - ✓ Формирование совместной проектной команды (**Комиссия по категорированию**)
   - ✓ Ознакомительный семинар (на вашей территории или в учебном центре)
2. Обследование (бизнес процессов и ИТ систем)
   - ✓ Изучение учредительных документов и пр.
   - ✓ Анкетирование / интервьюирование
   - ✓ Анализ и оценка защищенности инфраструктуры
3. Методологическая поддержка категорирования ОКИИ
4. Создание систем безопасности значимых ОКИИ
5. Оценка соответствия (при необходимости аттестация, сертификация, испытания)

# СПАСИБО ЗА ВНИМАНИЕ!

Мотылев Игорь
Руководитель группы аудита и консалтинга
+7 (985) 732 26 96
i.motylev@npo-echelon.ru

Эшелон

комплексная безопасность