Реализация Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». Взгляд субъекта критической информационной инфраструктуры

Бадеха Иван Александрович

Группа компаний Норильский никель

НОРНИКЕЛЬ

ГЕОЛОГОРАЗВЕДКА

НОРНИКЕЛЬ

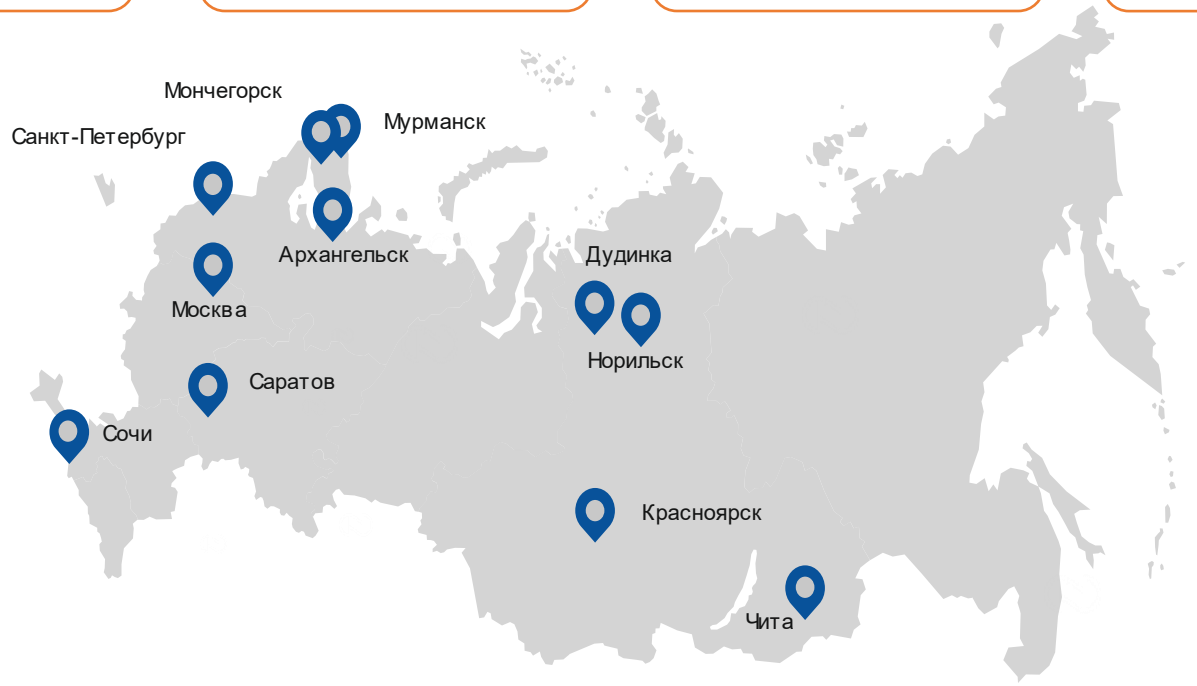
НАУЧНЫЕ КОМПЛЕКСЫ

ПРОИЗВОДСТВО

СБЫТОВАЯ СЕТЬ

ТРАНСПОРТ

ЭНЕРГЕТИКА



Нормативная база

Федеральный закон от 26.07.2017 № 187-ФЗ ≪О безопасности критической информационной инфраструктуры Российской Федерации≫

Федеральный закон от 26.07.2017 № 194-ФЗ ≪О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

Федеральный закон от 26.07.2017 № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры РФ и их значений»

Постановление Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Указ Президента Российской Федерации от 25.11.2017 № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю…»

Указ Президента РФ от 02.03.2018 № 98 «О внесении изменения в перечень сведений, отнесенных к государственной тайне…»

Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов…»

Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений…»

Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов…»

Информационное сообщение ФСТЭК России от 24.08.2018 № 240/25/3752 по вопросам представления перечней объектов

Права и обязанности субъекта КИИ (ст. 9 187-ФЗ)

НОРНИКЕЛЬ

Права (ч.1 ст. 9)

- Получать информацию от ФСТЭК России
- Получать информацию от ФСБ России
- **При наличии согласия ФСБ России** – за свой счет… средства обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ

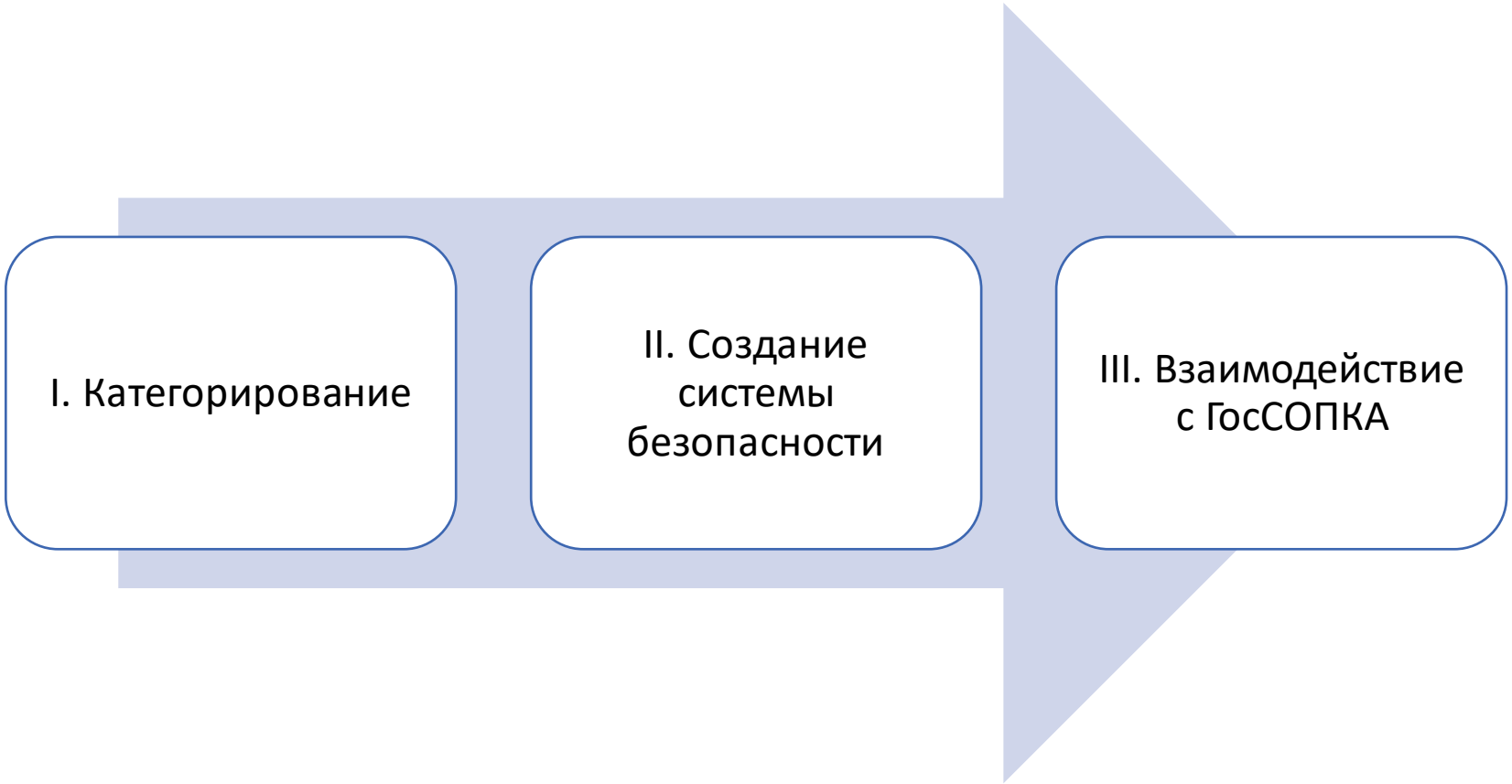
Общие обязанности (ч. 2 ст. 9):

- **Незамедлительно** информировать о КИ ФСБ России и ЦБ РФ* в установленном порядке
- Оказывать содействие должностным лицам ФСБ России
- В случае установки средств обнаружения, предупреждения и ликвидации последствий КА обеспечивать выполнение порядка, ТУ установки и эксплуатации, сохранность

+Обязанности владельцев ЗОКИИ (ч. 3 ст. 9)

- Соблюдать требования по обеспечению безопасности ЗОКИИ, установленные ФСТЭК России
- Выполнять предписания должностных лиц ФСТЭК России об устранении нарушений
- Реагировать на КИ в порядке, установленном ФСБ России, принимать меры по ликвидации последствий КА в отношении ЗОКИИ
- Обеспечивать беспрепятственный доступ должностным лицам ФСТЭК России в рамках мероприятий по государственному контролю

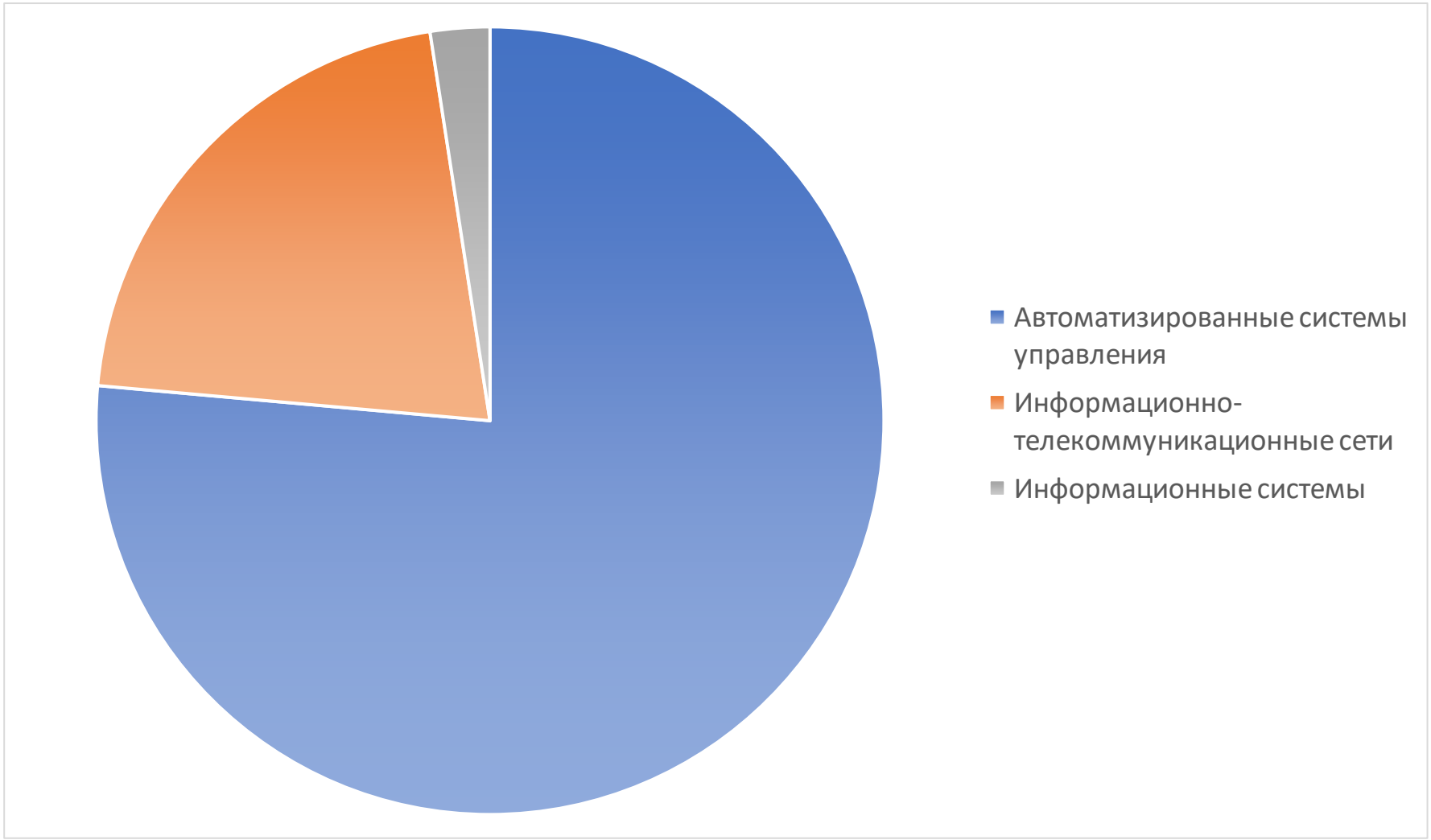
Обязательные мероприятия для субъекта КИИ



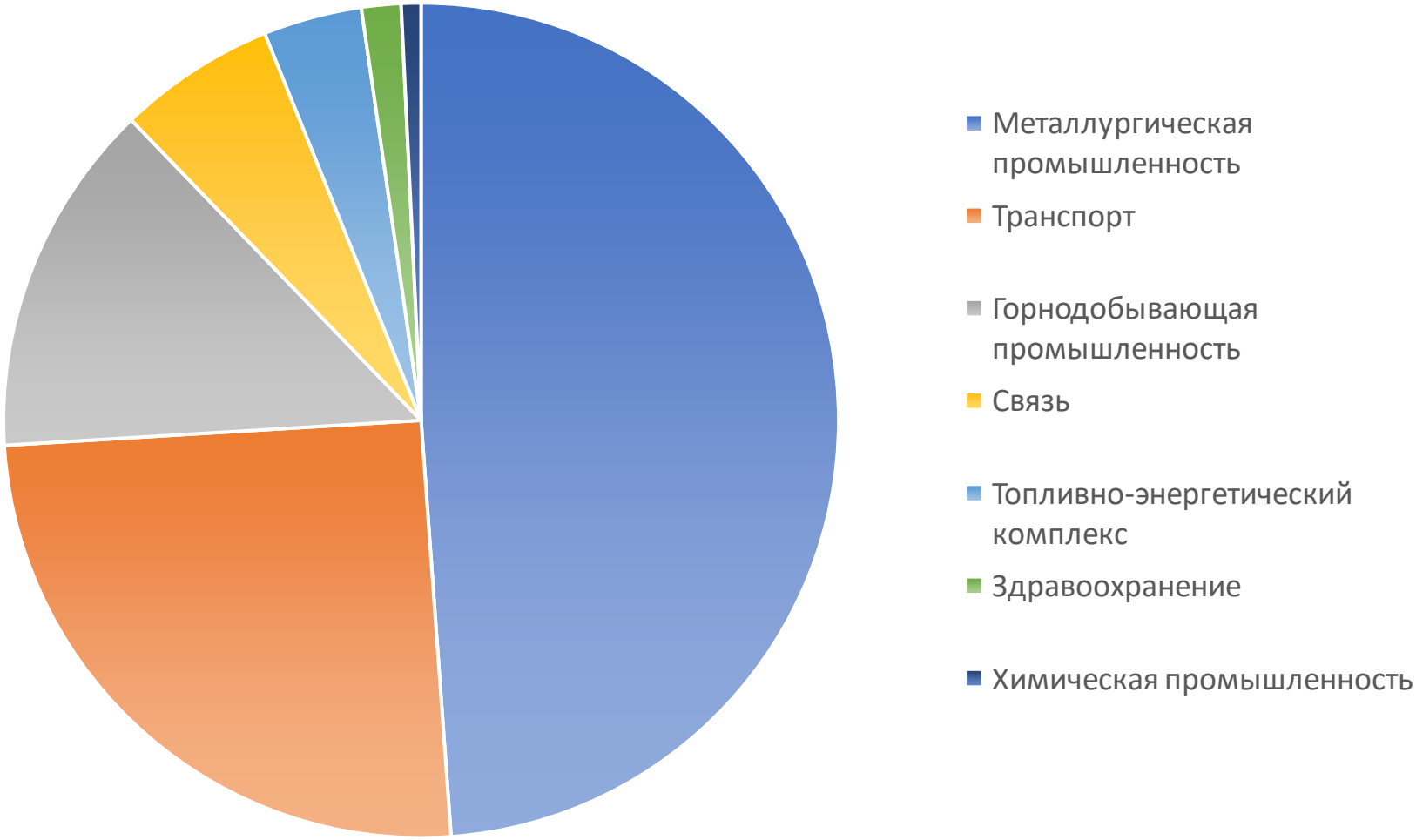
* Здесь и далее: КИИ = критическая информационная инфраструктура

I. Категорирование: применимость сфер 187-ФЗ

I. Категорирование: распределение значимых ОКИИ по типам



I. Категорирование: распределение значимых ОКИИ по отраслям



I. Категорирование: показатели

НОРНИКЕЛЬ

Социальная значимость

- **1. Причинение ущерба жизни и здоровью людей…**
- **2. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения…**
- 3. Прекращение или нарушение функционирования объектов транспортной инфраструктуры…
- 4. Прекращение или нарушение функционирования сети связи…
- 5. Отсутствие доступа к государственной услуге…

Политическая значимость

- 6. Прекращение или нарушение функционирования государственного органа…
- 7. Нарушение условий международного договора РФ…

Экономическая значимость

- 8. Возникновение ущерба СКИИ, который является гос. корпорацией, ГУП, МУП, гос. компанией, организацией с участием государства и (или) стратегическим АО, стратегическим предприятием…
- **9. Возникновение ущерба бюджетам РФ…**
- 10. Прекращение или нарушение проведения клиентами операций…

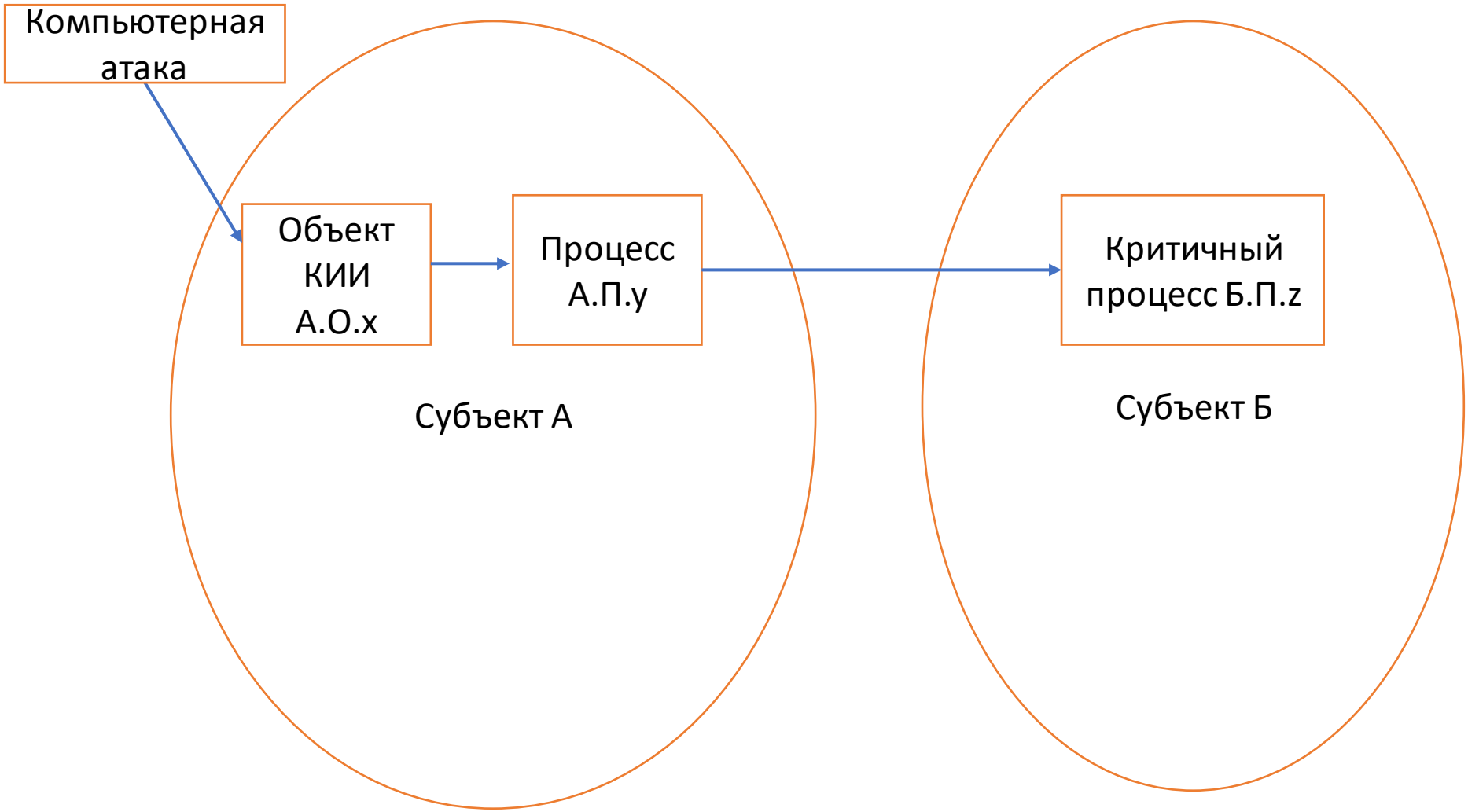
Экологическая значимость

- **11. Вредные воздействия на окружающую среду…**

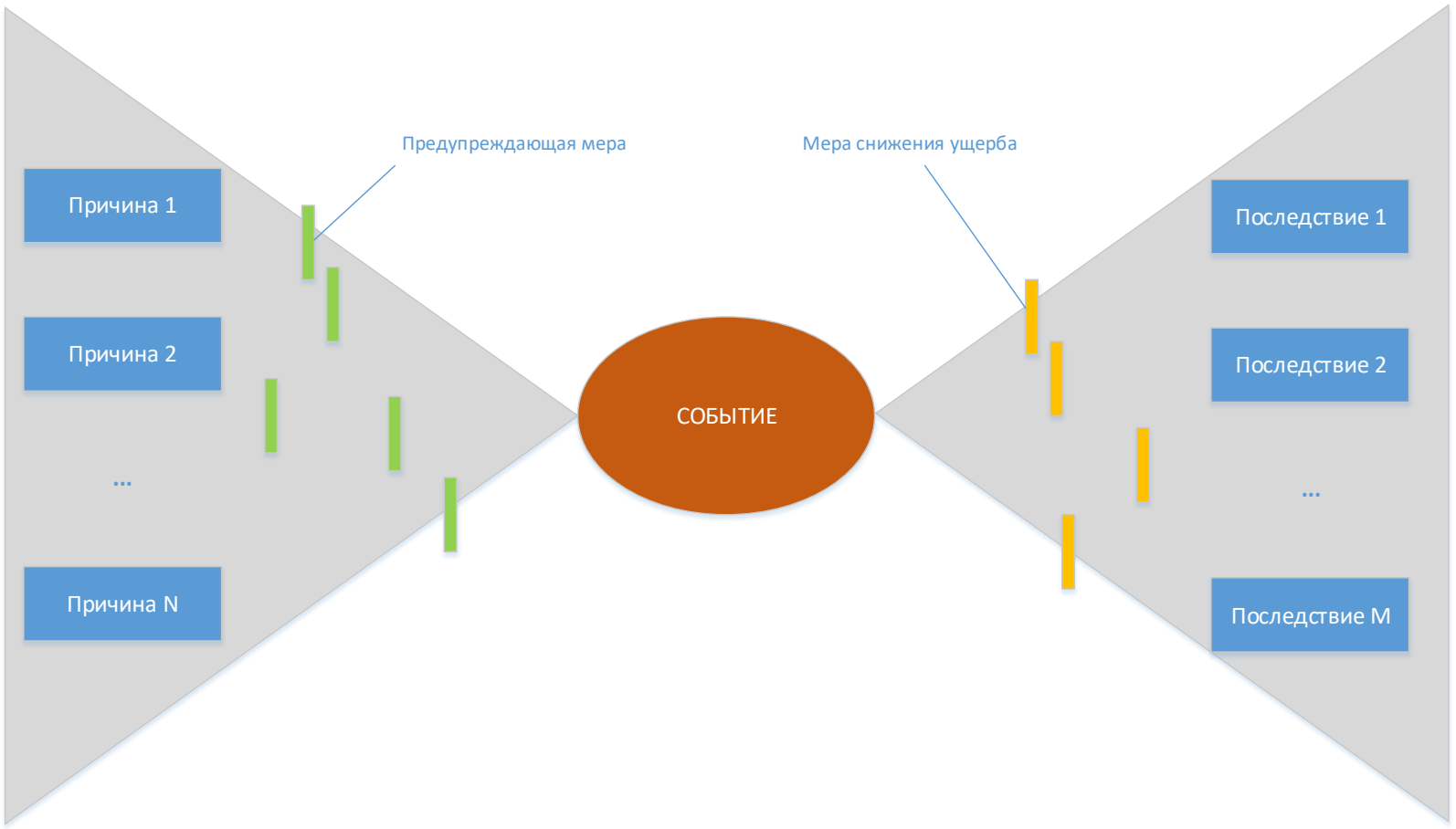
Значимость для обеспечения обороны страны, безопасности государства и правопорядка

- 12. Прекращение или нарушение функционирования пункта управления (СЦ)…
- 13. Снижение показателей гособоронзаказа…
- 14. Прекращение или нарушение функционирования ИС в области обеспечения обороны страны, безопасности государства и правопорядка…

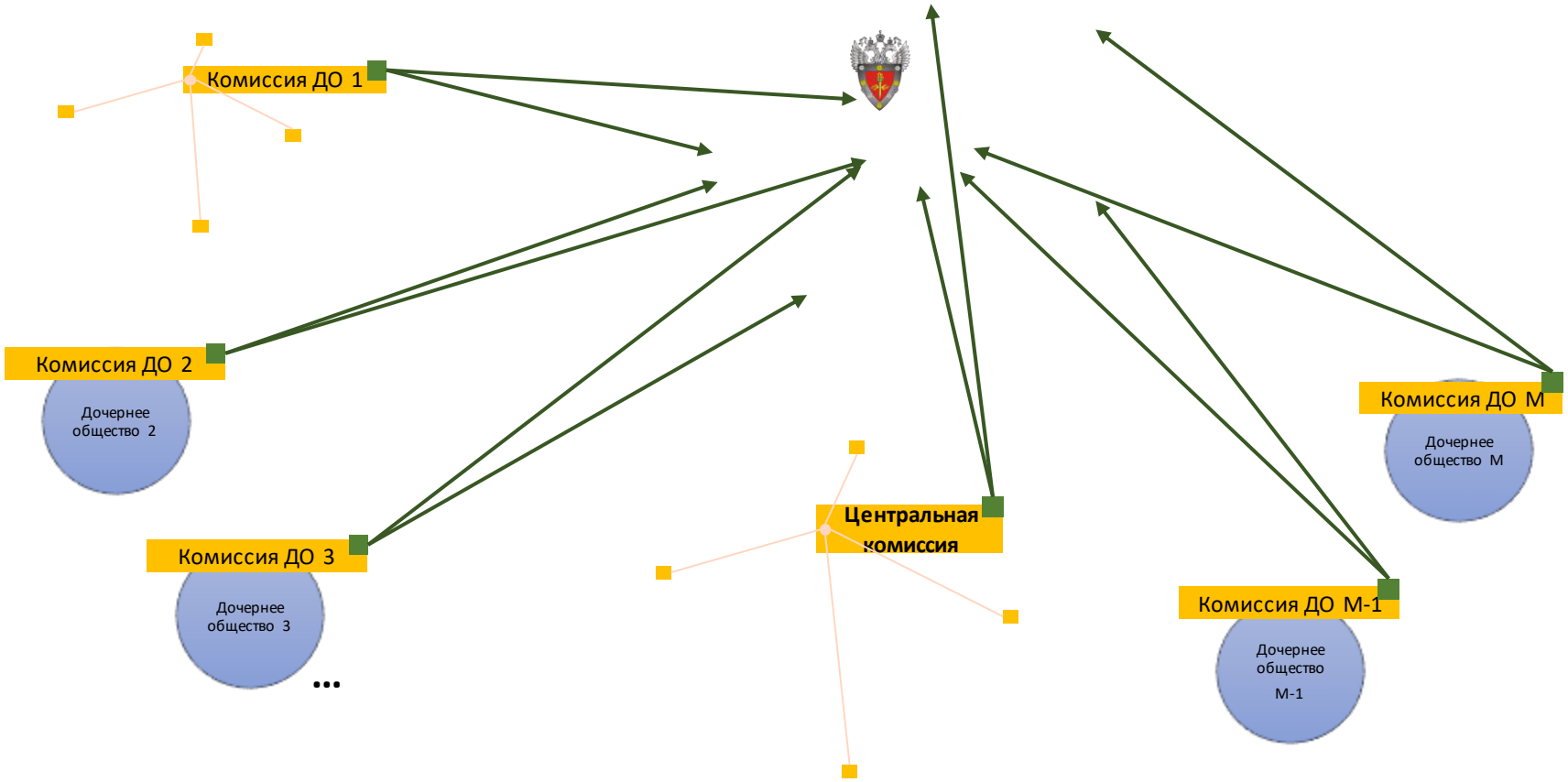
I. Категорирование: сложные сценарии атак



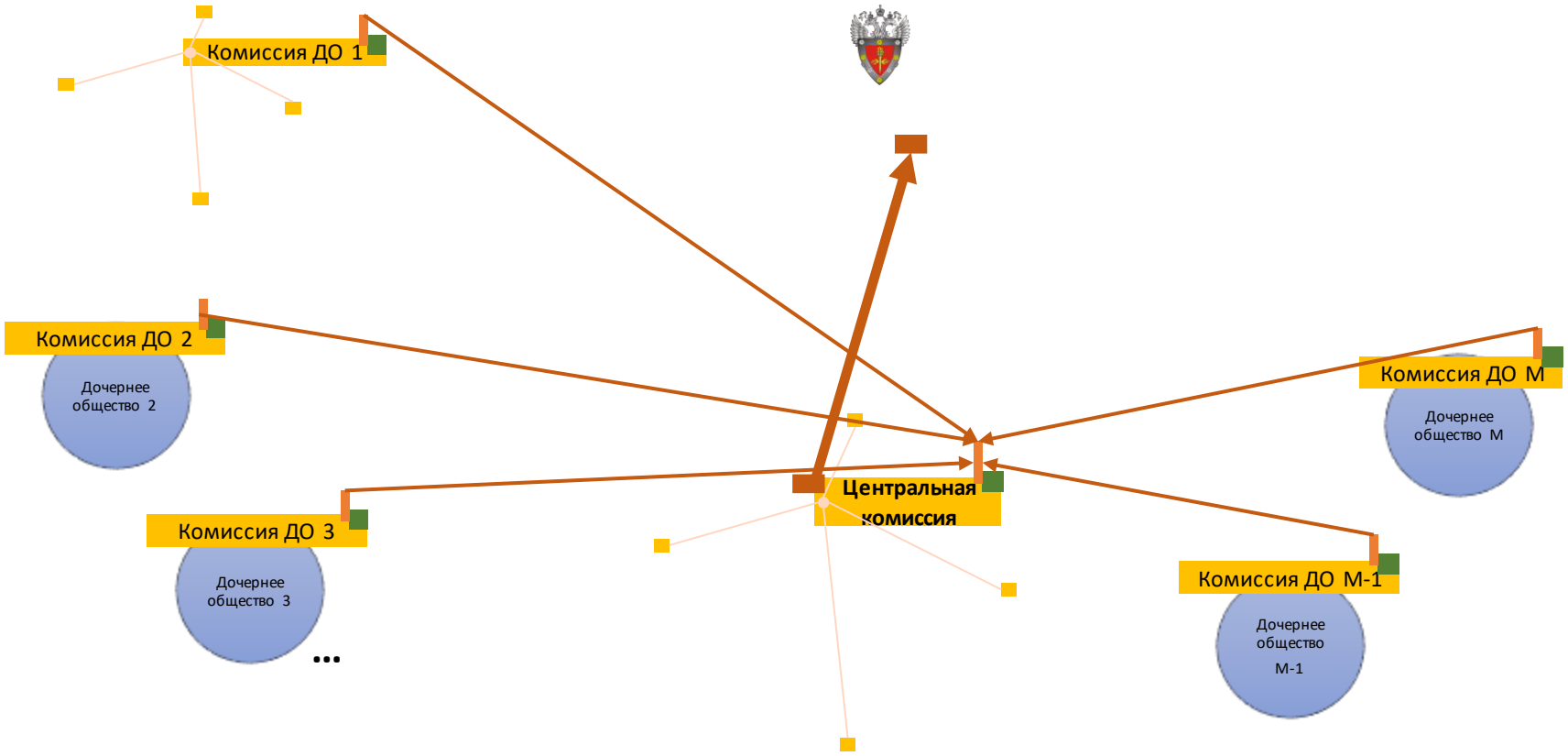
I. Категорирование: Анализ «галстук-бабочка»



I. Категорирование: Схема официального взаимодействия

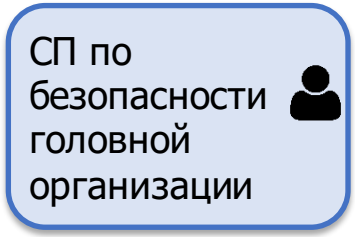


I. Категорирование: Схема рабочего взаимодействия



II. Система безопасности ЗОКИИ

II.1. Силы обеспечения безопасности КИИ



II.1. Силы обеспечения безопасности КИИ

НОРНИКЕЛЬ

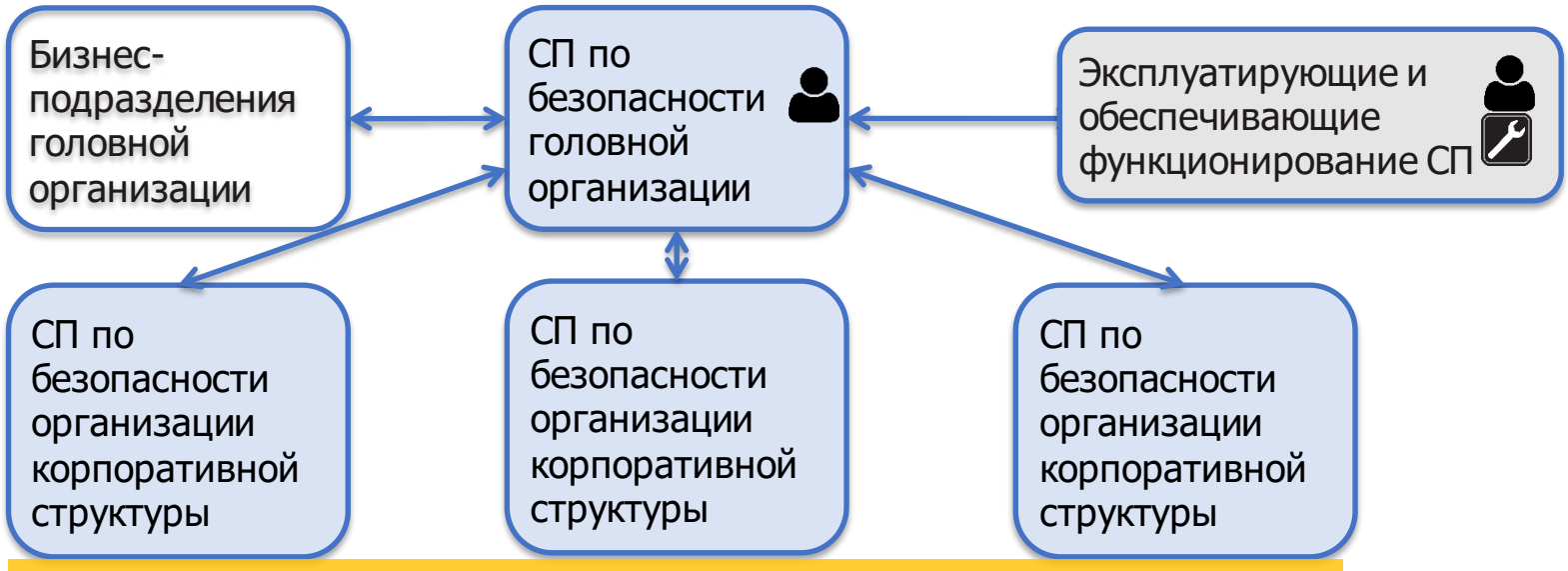
СП по безопасности головной организации

- курирует создание и реализацию сквозных процессов во всех организациях корпоративной структуры
- устанавливает метрики эффективности и результативности всех процессов менеджмента и обеспечения ИБ в группе компаний;
- осуществляет мониторинг и анализ инцидентов ИБ группы компаний
- осуществляет управление рисками ИБ группы компаний;
- выполняет роль ИБ-службы головной организации

II.1. Силы обеспечения безопасности КИИ

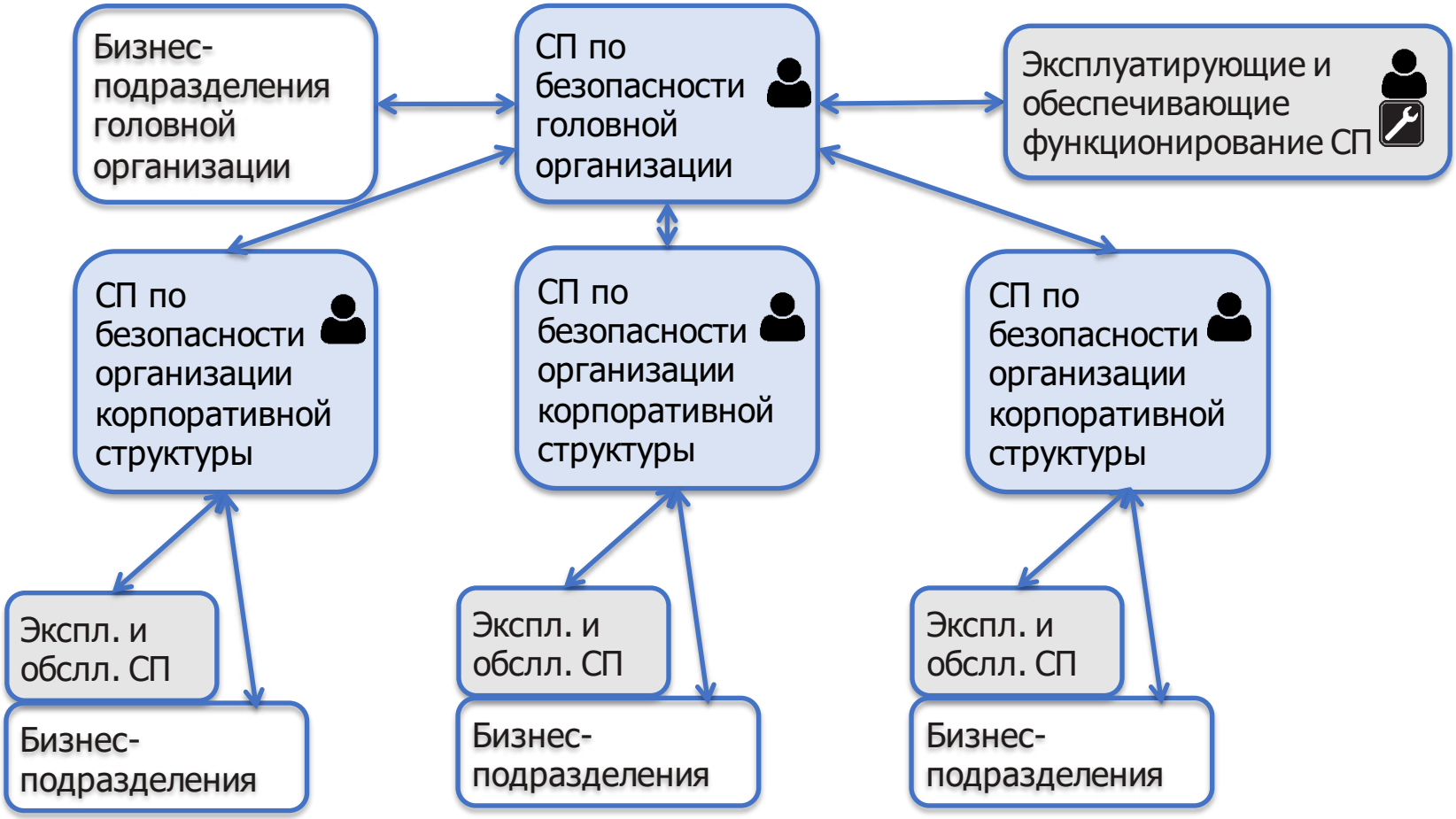
- курирует создание и реализацию сквозных процессов во всех организациях корпоративной структуры
- устанавливает метрики эффективности и результативности всех процессов менеджмента и обеспечения ИБ в группе компаний;
- осуществляет мониторинг и анализ инцидентов ИБ группы компаний
- осуществляет управление рисками ИБ группы компаний;
- выполняет роль ИБ-службы головной организации

II.1. Силы обеспечения безопасности КИИ



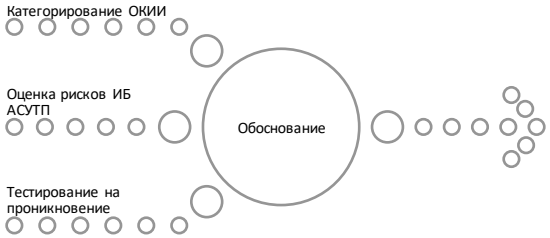
- выполняет функции исполнителя процедур в рамках процессов менеджмента и обеспечения ИБ в компании;
- осуществляет реагирование на инциденты ИБ компании
- формирует отчетность перед СП по безопасности головной организации об эффективности и результативности всех процессов менеджмента и обеспечения ИБ

II.1. Силы обеспечения безопасности КИИ



II.2. Средства обеспечения безопасности КИИ: порядок создания

II.2. Средства обеспечения безопасности КИИ: порядок создания



Предприятие 1

1.Обследование

2.Проектирование

3.Ввод в действие

Предприятие 2

Обследование

Проектирование

Ввод в действие

...

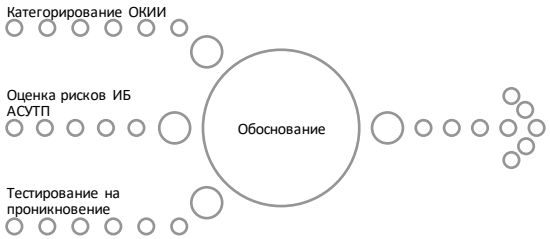
Предприятие n

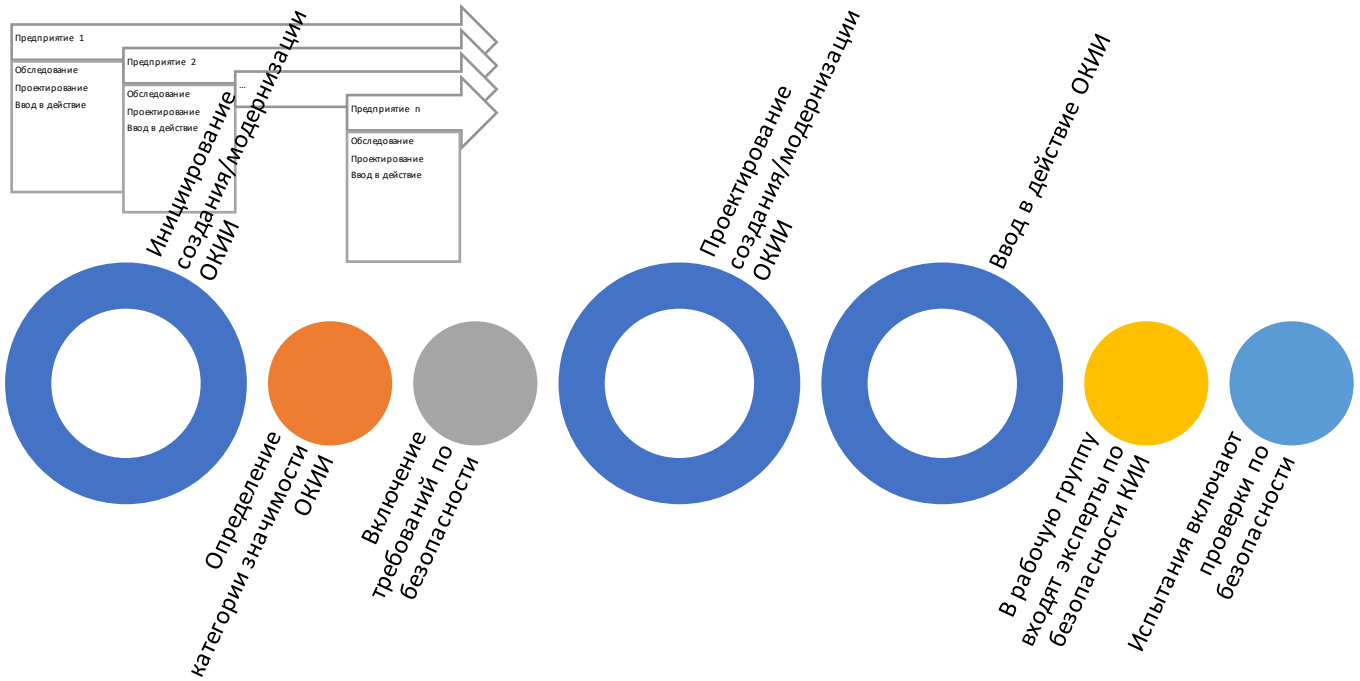
Обследование

Проектирование

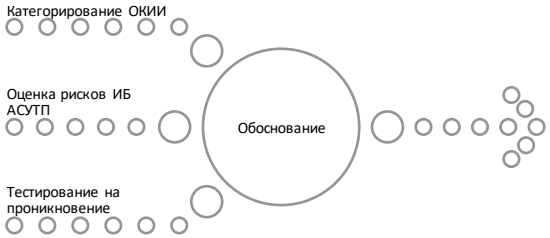
Ввод в действие

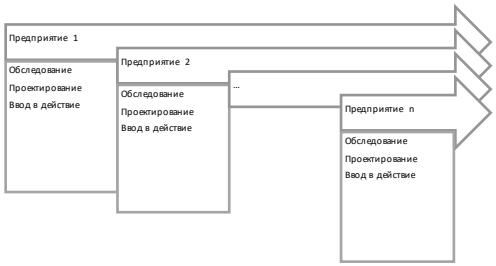
II.2. Средства обеспечения безопасности КИИ: порядок создания

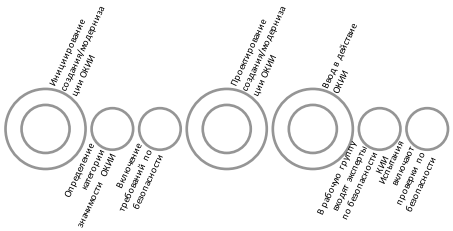




II.2. Средства обеспечения безопасности КИИ: порядок создания





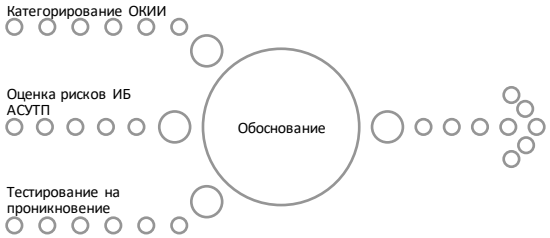


Оценка соответствия средств защиты информации

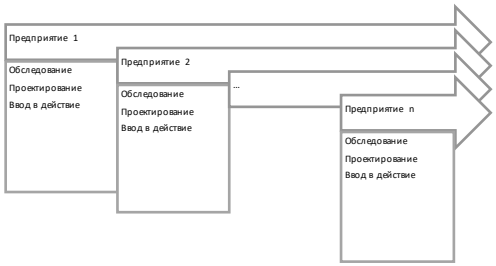
Оценка соответствия системы в целом

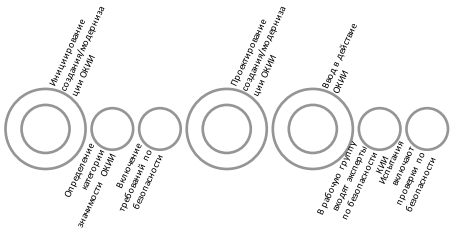
Комплексные испытания централизованной системы защиты

II.2. Средства обеспечения безопасности КИИ: порядок создания



Актуален вопрос формирования, апробирования и подтверждения легитимности методик испытаний!





Оценка соответствия средств защиты информации

Оценка соответствия системы в целом

Комплексные испытания централизованной системы защиты

III. ГосСОПКА: нормативная база

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утверждены Президентом РФ 3 февраля 2012 г., № 803)

Указ Президента РФ от 15.01.2013 № 31с «О создании государственной системы…»

Концепция государственной системы… (утверждена Президентом РФ 12 декабря 2014 г. № К 1274)

Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам»

Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой … и Порядка представления информации…»

Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации…»

Методические рекомендации:

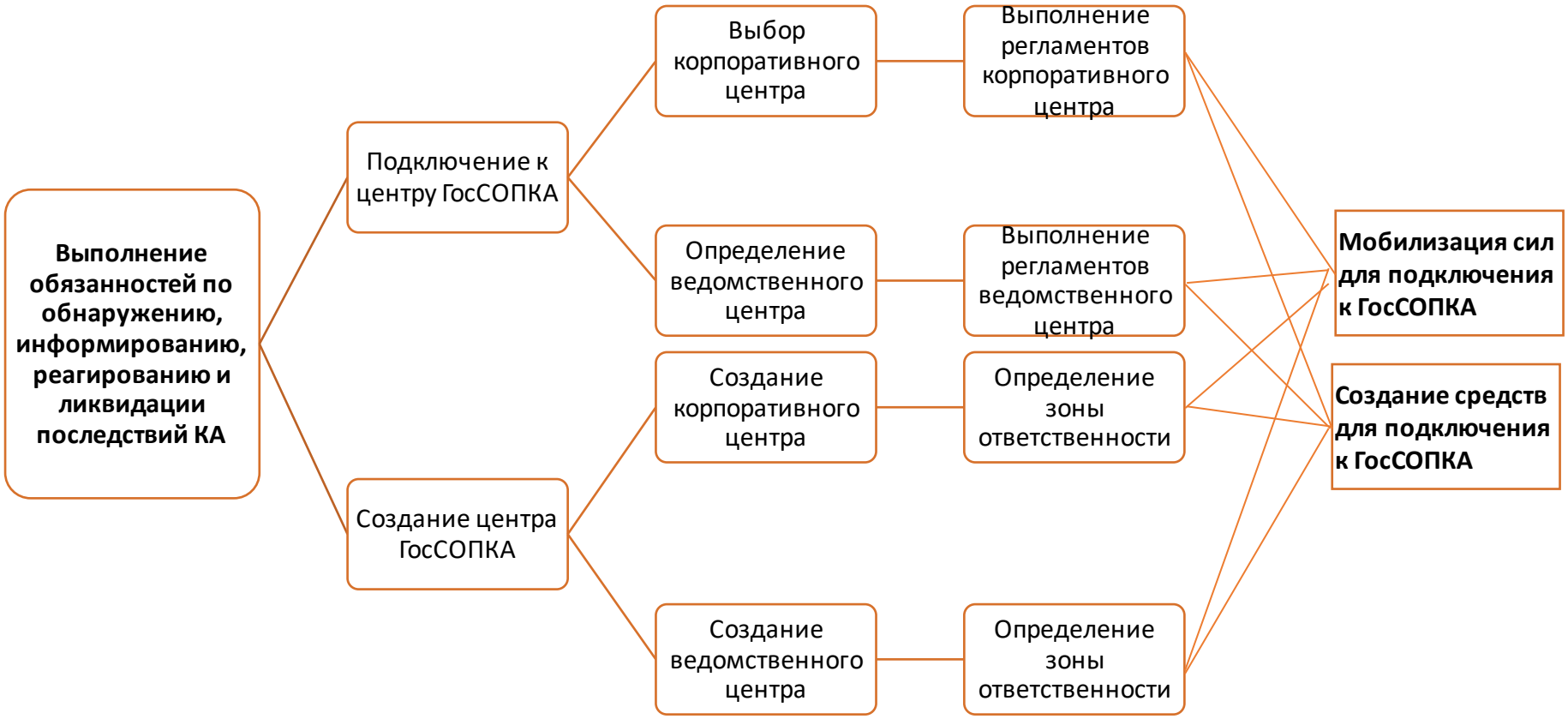
- по созданию ведомственных и корпоративных центров ГосСОПКА
- по обнаружению компьютерных атак
- по установлению причин и ликвидации последствий компьютерных инцидентов
- о проведению мероприятий по оценке степени защищенности от компьютерных атак

Временный порядок включения корпоративных центров в государственную систему…

Требования к подразделениям и должностным лицам субъектов государственной системы…

Регламент взаимодействия подразделений Федеральной службы безопасности Российской Федерации и организации при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак

III. ГосСОПКА: варианты взаимодействия



Заключение

НОРНИКЕЛЬ

Ценность результатов мероприятий 187-ФЗ для ИБ и бизнеса

- Идентификация защищаемых активов
- Оценка рисков ИБ и приоритизация затратных мероприятий

Совпадение интересов государства и бизнеса

- Тесное рабочее взаимодействие в рамках профильных сообществ
- Открытое взаимодействие с регулятором
- Совместная плодотворная работа в направлении укрепления безопасности страны в киберпространстве

Точки приложения усилий

- Необходимо создание методик по испытанию средств защиты информации в составе системы безопасности ЗОКИИ

НОРНИКЕЛЬ

СПАСИБО ЗА ВНИМАНИЕ

Бадеха Иван Александрович
badekhaia@nornik.ru