

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В РЕАЛИЯХ БИЗНЕС-ТРЕБОВАНИЙ РФ

ТЕМА 3

Риски ИБ. COMPLAINTS.

Спикер: Ануфриев Иван



ЗАНЯТИЕ 3.1

Обзор ключевых НПА по ИБ. Корпоративный комплаенс



Условное разделение информации. «Метки» на слайдах *

«Машина-времени-Time-machine» Возвращаемся и освежаем знания с прошлых занятий.		«Назад в будущее» Анонсируем то, что будет сказано на следующих занятиях	Метки по Времени
			
Рабочий «экспертный» инструментарий «Expert tools»	Примеры рабочих документов, лучшие приемы, практики и примеры использования. «Best practice»		Метки по используемым инструментам и практикам
[EXPERT TOOLS] 	[BEST PRACTICE]		
Полезные мысли и выводы «Инсайты»	Соответствие требованиям, нормативная база и полезные формы по НПА	В нашем курсе, отдельно выделяется информация, относящаяся к типу «непрерывность бизнеса»	Метки по типу информации
[INSIGHTS]	[COMPLIANCE] 	[BUSINESS CONTINUITY]	



ОСНОВНЫЕ РАССМАТРИВАЕМЫЕ ВОПРОСЫ ЗАНЯТИЯ

ВОПРОС 1.1.

Общая
«раскадровка» по
некоторым НПА.
ПДн, ГИС, КИИ

ВОПРОС 1.2.

Комплаенс-карта
по КИИ

ВОПРОС 1.3.

Основные виды
информации

ВОПРОС 1.4

Основные
регуляторы по ИБ
и их функции

ВОПРОС 1.5

Основные НПА в
одном документе

1

Ч
А
С
Т
Ь

ВОПРОС 2.1.

ПОСТРОЕНИЕ
СТРУКТУРЫ НПА В
ОРГАНИЗАЦИИ

ВОПРОС 2.2.

СХЕМА НПА В
СОВРЕМЕННОЙ
ОРГАНИЗАЦИИ

ВОПРОС 2.3.

УРОВНИ НПА В
ОРГАНИЗАЦИИ

ВОПРОС 2.4.

СТРУКТУРА НПА
ВЕРХНЕГО УРОВНЯ

ВОПРОС 2.5.

КАРТА ПРОЦЕССОВ
УПРАВЛЕНИЯ И
ОБЕСПЕЧЕНИЯ ИБ

2

Ч
А
С
Т
Ь



ОСНОВНЫЕ РАССМАТРИВАЕМЫЕ ВОПРОСЫ ПЕРВОЙ ЧАСТИ ЗАНЯТИЯ

ВОПРОС 1.1.

**Общая
«раскадровка» по
некоторым НПА.
ПДн, ГИС, КИИ**

ВОПРОС 1.2.

**Комплаенс-карта
по КИИ**

ВОПРОС 1.3.

**Основные виды
информации**

ВОПРОС 1.4

**Основные
регуляторы по ИБ
и их функции**

ВОПРОС 1.5

**Основные НПА в
одном документе**



ОБЩАЯ СТРУКТУРА НПА РФ. ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ



ЕСТЬ ГИС ? ПДН ? МЫ ПОПАДАЕМ ПОД СФЕРУ КИИ?

ПДН

Если в организации есть персональные данные (перечень основных НПА)

Федеральный закон № 152

База

Постановление Правительства РФ № 1119

Приказа ФСТЭК №21

ГИС

Если в организации есть государственные информационные системы (перечень основных НПА)

Федеральный закон №149

база

Приказ ФСТЭК РФ №17

КИИ

Если организация является субъектом критической информационной инфраструктуры

Федеральный закон №187

база

Постановление Правительства №127

Приказ ФСТЭК РФ № 239



ПДН

Если в организации есть
персональные данные (перечень
основных НПА)

Федеральный закон № 152
База

Постановление Правительства РФ № 1119

Приказа ФСТЭК №21

Внесение
изменений
от 06 июля
2022 г.

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в Федеральный закон
«О персональных данных», отдельные законодательные акты
Российской Федерации и признании утратившей силу части
четырнадцатой статьи 30 Федерального закона
«О банках и банковской деятельности»

Принят Государственной Думой

6 июля 2022 года

Одобрено Советом Федерации

8 июля 2022 года

Статья 1

Внести в Федеральный закон от 27 июля 2006 года № 152-ФЗ
«О персональных данных» (Собрание законодательства Российской
Федерации, 2006, № 31, ст. 3451; 2010, № 27, ст. 3407; 2011, № 31, ст. 4701;
2013, № 14, ст. 1651; № 51, ст. 6683; 2014, № 23, ст. 2927; № 30, ст. 4243;
2016, № 27, ст. 4164; 2017, № 9, ст. 1276; № 27, ст. 3945; № 31, ст. 4772;
2018, № 1, ст. 82; 2019, № 52, ст. 7798; 2020, № 17, ст. 2701; № 50, ст. 8074;
2021, № 1, ст. 54, 58; № 24, ст. 4188; № 27, ст. 5159) следующие изменения:

1) статью 1 дополнить частью 1¹ следующего содержания:



2 100068 24642 1



ПДН

Если в организации есть персональные данные (перечень основных НПА)

Федеральный закон № 152

База

Постановление Правительства РФ № 1119

Приказа ФСТЭК №21

ГИС

Если в организации есть государственные информационные системы (перечень основных НПА)

Федеральный закон №149

база

Приказ ФСТЭК РФ №17

КИИ

Если организация является субъектом критической информационной инфраструктуры

Федеральный закон №187

база

Постановление Правительства №127

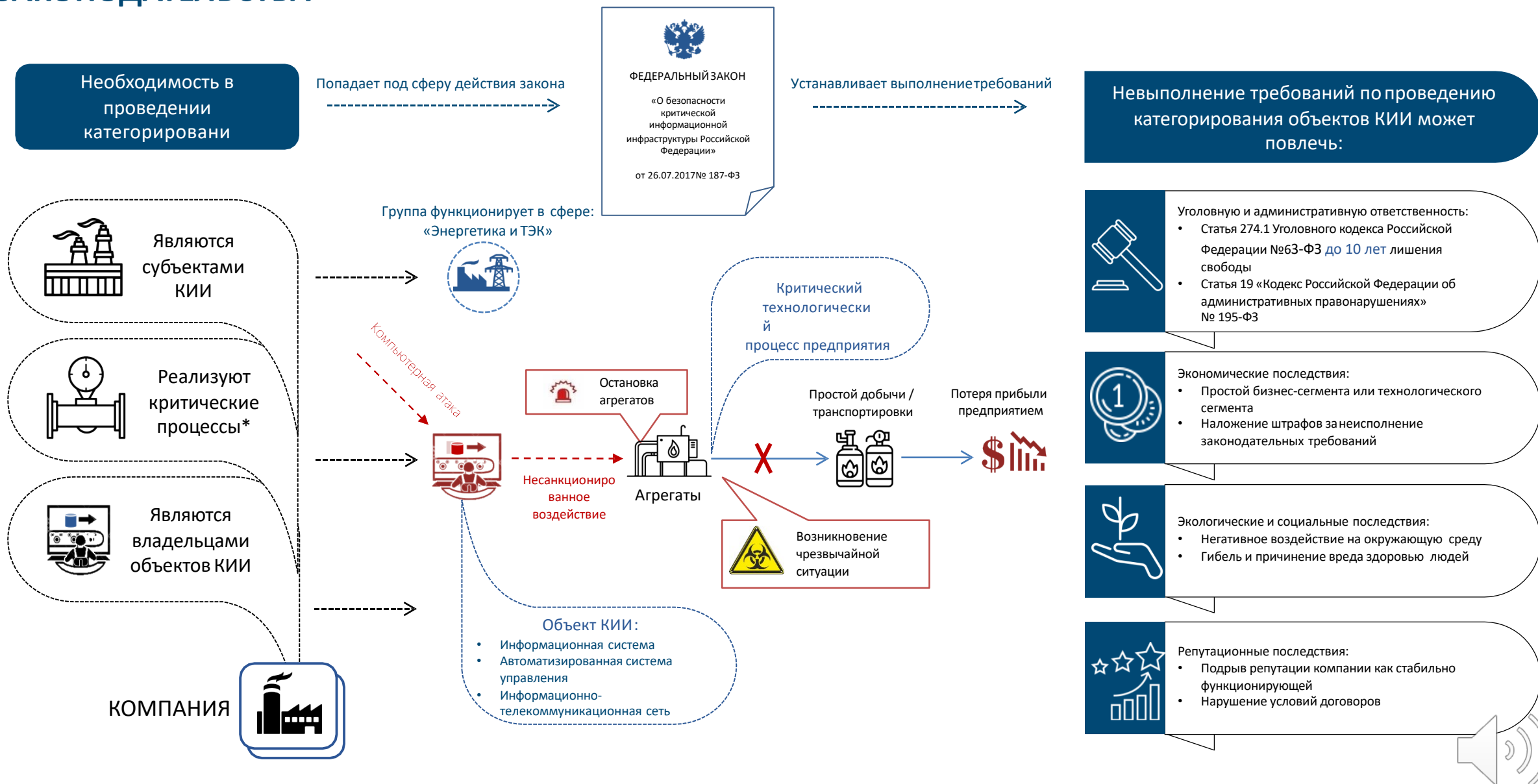
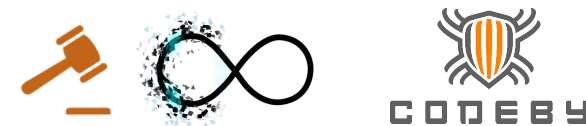
Приказ ФСТЭК РФ № 239



ПРИМЕРЫ ГИС *и нпа* (ПРОДОЛЖЕНИЕ)



КОМПАЕНС КАРТА ПО КИИ – ОБЕСПЕЧЕНИЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА



* Выявление критических процессов основывается на результатах оценки последствий рисков ИБ

УЧИМСЯ ПОЛЬЗОВАТЬСЯ РАБОЧИМ ДОКУМЕНТОМ ДЛЯ РАСЧЕТА ТРУДОЗАТРАТ ДЛЯ ОБЕСПЕЧЕНИЯ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА ПО КИИ. СОСТАВ РАБОТ ПО КИИ



СОСТАВ ЭТАПОВ	
№ этапа	Наименование работ
1	Обследование информационной инфраструктуры Заказчика
2	Разработка организационной структуры и архитектуры ведомственного сегмента ГосСОПКА
3	Установка и настройка технических средств
4	Разработка организационно-методического обеспечения
5	Ввод в эксплуатацию ведомственного сегмента ГосСОПКА
ИТОГО работы:	



Состав работ ГосСОПКА.xlsx
(документ в приложении)

Более подробно тему КИИ мы рассмотрим на следующих занятиях

№ ЭТАПА	НАИМЕНОВАНИЕ РАБОТ	ДЕТАЛИЗАЦИЯ РАБОТ ПО КАЖДОМУ ЭТАПУ	ПРОГНОЗ ТРУДОЗАТРАТ	
			Трудозатраты (человеко/дни)	Тр.часы
1	Обследование информационной инфраструктуры Заказчика			
1.1	Планирование работ по обследованию информационной инфраструктуры Заказчика	Разработка Плана обследования, включающего перечень работ, ответственных и сроки выполнения		0
1.2	Обследование информационной инфраструктуры Заказчика	Обследование включает: - сбор сведений об информационной инфраструктуре Заказчика (архитектуре сети, применяемых ИТ, составе и размещении программно-аппаратных компонентов); - сбор и анализ сведений о составе применяемых Заказчиком для обнаружения компьютерных атак, реагирования на инциденты безопасности сил и средств, включая информацию о штатной численности и подготовки персонала в области обнаружения, предупреждения и ликвидации последствий компьютерных атак; - сбор информации об информационных ресурсах, которые планируется включить в зону ответственности ведомственного сегмента ГосСОПКА; - сбор информации о применяемых мерах защиты информационных ресурсов; - анализ ОРД, регламентирующих требования по обеспечению ИБ информационных ресурсов.		0



И КТО БУДЕТ РЕГУЛЯТОРОМ ДЛЯ НАС ?



ФСБ России

Федеральная служба безопасности Российской Федерации

- Контроль за соблюдением лицензионных требований в части криптографии
- Проведение сертификации средств защиты
- Управление ввозом/вывозом специализированных технических средств



ФСТЭК России

Федеральная служба по техническому и экспортному контролю

- Контроль за соблюдением лицензионных требований по ТЗКИ
- Контроль за импортом/экспортом товаров, услуг, информации
- Проведение независимой идентификационной экспертизы товаров и технологий в целях экспортного контроля



Роскомнадзор

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

- Защита и поддержка прав субъектов персональных данных
- Поддержка реестра федеральных государственных информационных систем
- Поддержка реестра операторов персональных данных



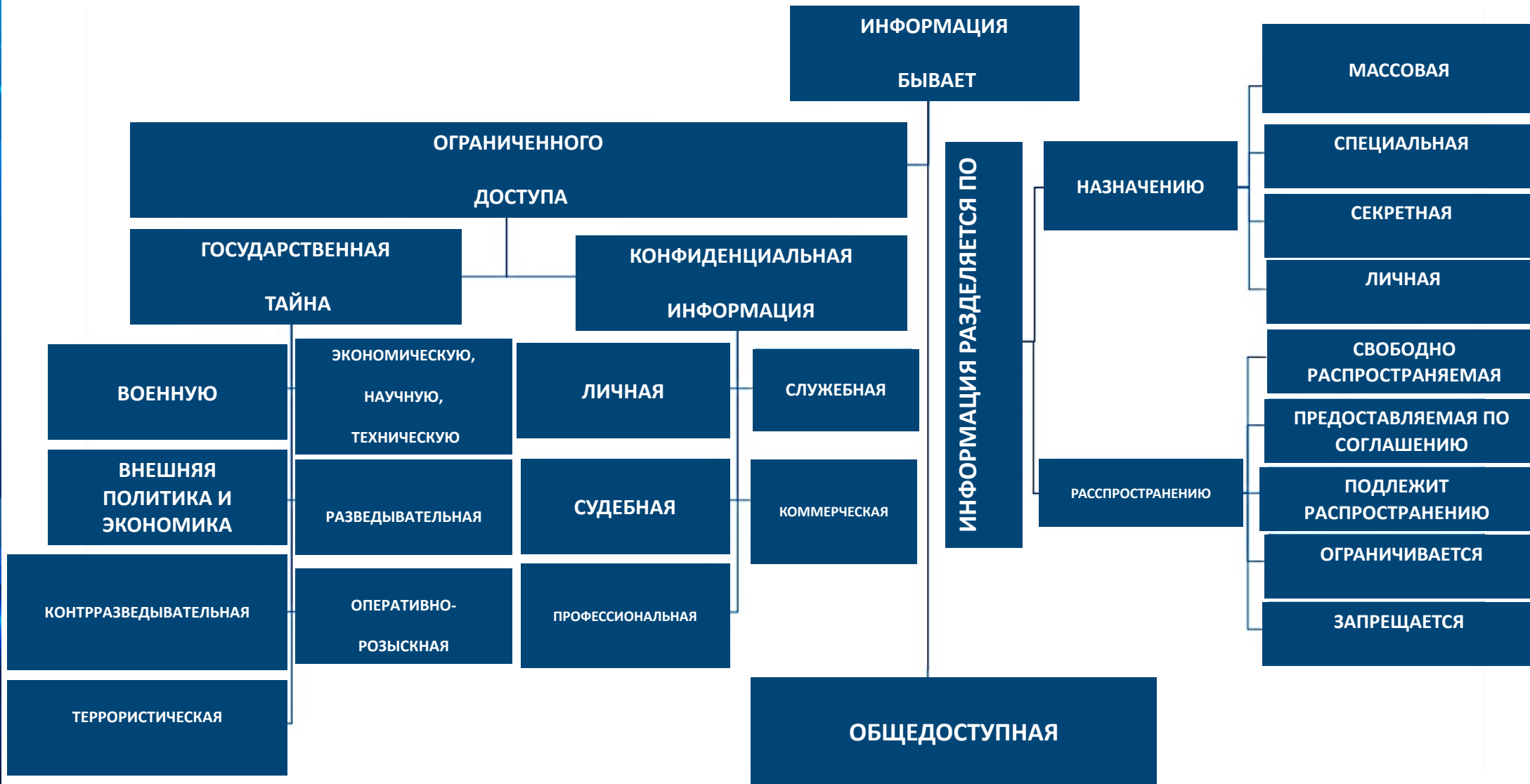
Минцфры России

Министерство цифрового развития, связи и массовых коммуникаций

- Аккредитация удостоверяющих центров
- Ограничение доступа к копиям заблокированных сайтов
- Развитие нормативно-правовой базы в сфере связи, информационных технологий и массовых коммуникаций



КАКИЕ ВИДЫ ИНФОРМАЦИИ ?



УЧИМСЯ ПОЛЬЗОВАТЬСЯ «РАБОЧИМ ИНСТРУМЕНТОМ».

ОСНОВНЫЕ НПА И СТАНДАРТЫ ПО ИБ (360 +) В ОДНОМ ДОКУМЕНТЕ



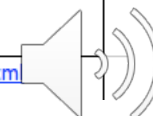
СОСТАВ ДОКУМЕНТА

Листы
Межд ISO
Межд NIST
ФедЗ "ИБ и ЗИ"
ФедЗ "Служебная тайна"
ФедЗ "ПДн"
ФедЗ "ГИС"
ФедЗ "ТехничЗ"
ФедЗ ГОСТы РФ
ФедЗ РД СЗИ
ФедЗ СКЗИ
НПА Москвы
НПА ДИТ Москвы
"Ворчалка"
Критерии ФСТЭК 17 К2 и У32
Критерии ГОСТ 27001 2006
Критерии ISO 27001 2013
Критерии Доп!Орг!Процессы



Свод НПА по критериям.xlsx
(документ в приложении)

КАТЕГОРИЯ	ОФИЦИАЛЬНОЕ	ДЕТАЛИЗАЦИЯ ОСНОВНЫХ ПОЛОЖЕНИЙ НПА	URL АКТУАЛЬНОГО
9	Акты Правительства Постановление Правительства РФ от 06.07.2008 №512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных"	Установлены требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. Требования распространяются на машиночитаемые носители информации (в том числе магнитные и электронные, за исключением бумажных), на которых осуществляются запись и хранение биометрических персональных данных.	http://www.ig.it, 2008/07/11/trebovaniya-dok.html
10	Акты Правительства Постановление Правительства РФ от 15.09.2008 №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"	Определены особенности обработки персональных данных, осуществляемой без использования средств автоматизации. При этом действия с такими сведениями в отношении каждого из лиц производятся при непосредственном участии человека. Предусмотрено, что в таком случае данные должны отделяться от другой информации (путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм). При использовании типовых форм документов, в которые может быть включена информация о лице, необходимо соблюдать определенные условия. Так, если нужно письменное согласие гражданина на работу с его данными, типовая форма должна иметь поле, в котором он может поставить отметку о своем согласии на обработку его сведений без применения автоматизации.	http://www.rg.ru/2008/09/24/dannye-obrabotka-dok.html
	Акты Правительства Постановление Правительства РФ от 21.03.2012 N 344 "Об утверждении Перечня мер, направленных на обеспечение выполнения обязанностей, возложенных на органы государственной власти в сфере защиты информации"	Утвержден Перечень мер, направленных на обеспечение выполнения обязанностей, возложенных на органы государственной власти в сфере защиты информации.	http://www.rg.ru/2012/03/30/dannie-dok.html



ОСНОВНЫЕ РАССМАТРИВАЕМЫЕ ВОПРОСЫ ВТОРОЙ ЧАСТИ ЗАНЯТИЯ

ВОПРОС 2.1.

**ПОСТРОЕНИЕ
СТРУКТУРЫ НПА В
ОРГАНИЗАЦИИ**

ВОПРОС 2.2.

**СХЕМА НПА В
СОВРЕМЕННОЙ
ОРГАНИЗАЦИИ**

ВОПРОС 2.3.

**УРОВНИ НПА В
ОРГАНИЗАЦИИ**

ВОПРОС 2.4.

**СТРУКТУРА НПА
ВЕРХНЕГО УРОВНЯ**

ВОПРОС 2.5.

**КАРТА ПРОЦЕССОВ
УПРАВЛЕНИ И
ОБЕСПЧЕНИЯ ИБ**



С ЧЕГО НАЧИНАЕТСЯ ПОСТРОЕНИЕ МОДЕЛИ ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНОЙ ДОКУМЕНТАЦИИ ?

1



Направления развития ИБ

Обследование информационной инфраструктуры компании, определение основных направлений развития ИБ с учетом требований нормативных документов, стандартов ИБ, лучших практик, категорий значимости объектов КИИ

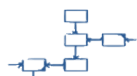
2



Программа проектов ИБ

Определение портфеля проектов и разработка верхнеуровневой архитектуры комплексной системы ИБ

3



Карта процессов ИБ

Определение перечня и области внедрения процессов ИБ, разработка карты процессов управления и обеспечения ИБ

4



Оргструктура комплексной системы ИБ

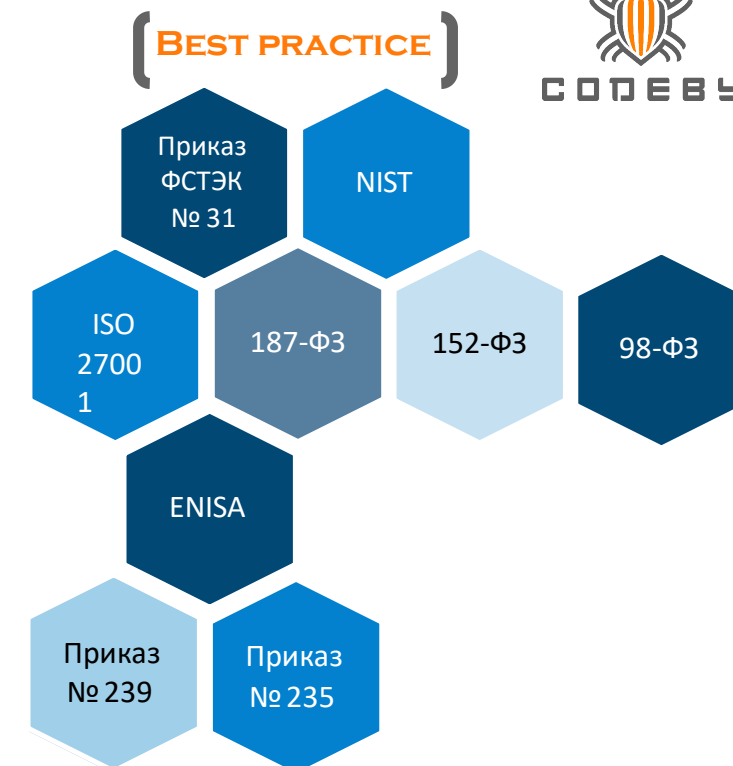
Разработка организационной структуры комплексной системы ИБ, определение численности и ролей персонала в области ИБ

5

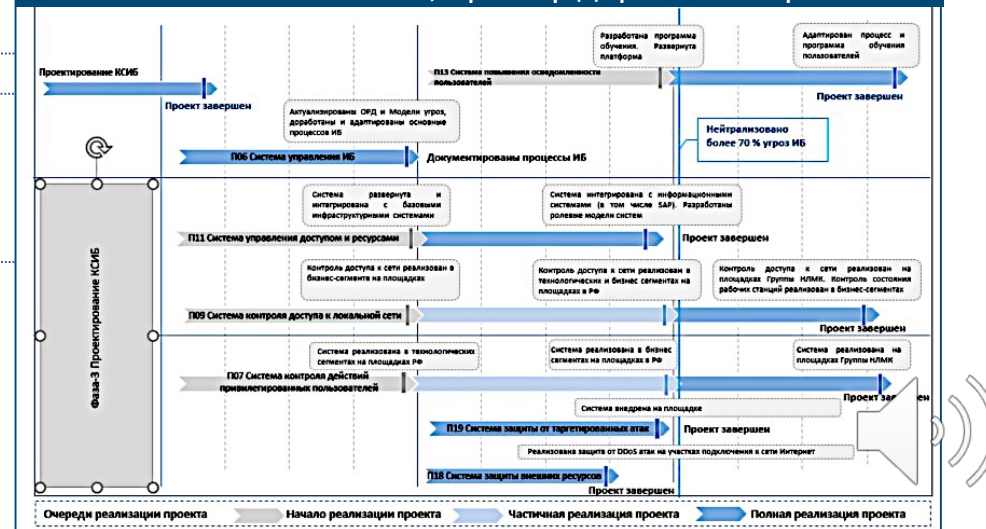


Презентация Стратегии ИБ

Презентация руководству Стратегии развития информационной безопасности, планируемых сроков и стоимости её реализации, снижаемых за счет реализации стратегии рисков ИБ

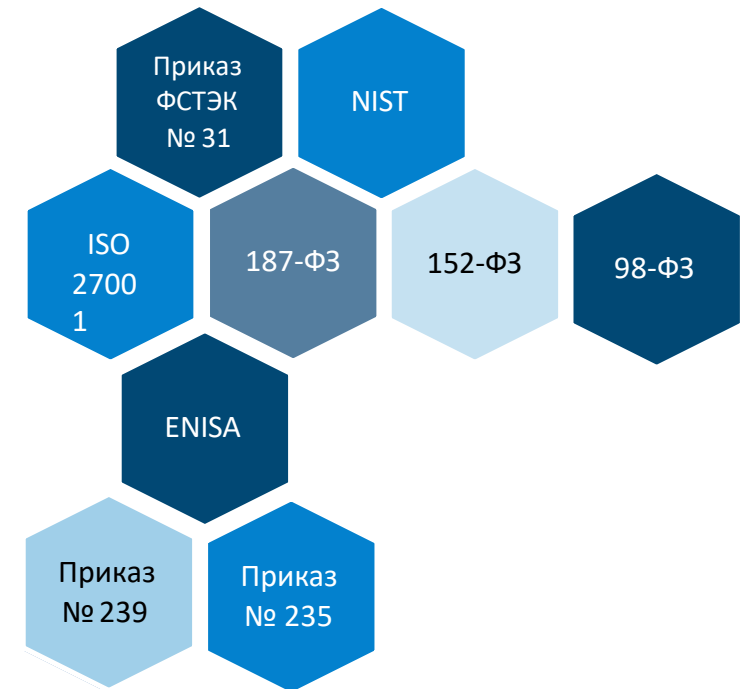


СТРАТЕГИЯ РАЗВИТИЯ ИБ, пример дорожной карты



1 |

Направления
развития ИБ



1



Направления
развития ИБ

Методологии в нашем случае:

*Какие гибкие методологии для
определения программы проектов ?*

2



Программа
проектов ИБ

Уровни:

*Какие бывают
уровни
безопасности (в
нашем случае для
СМИБ) ?*

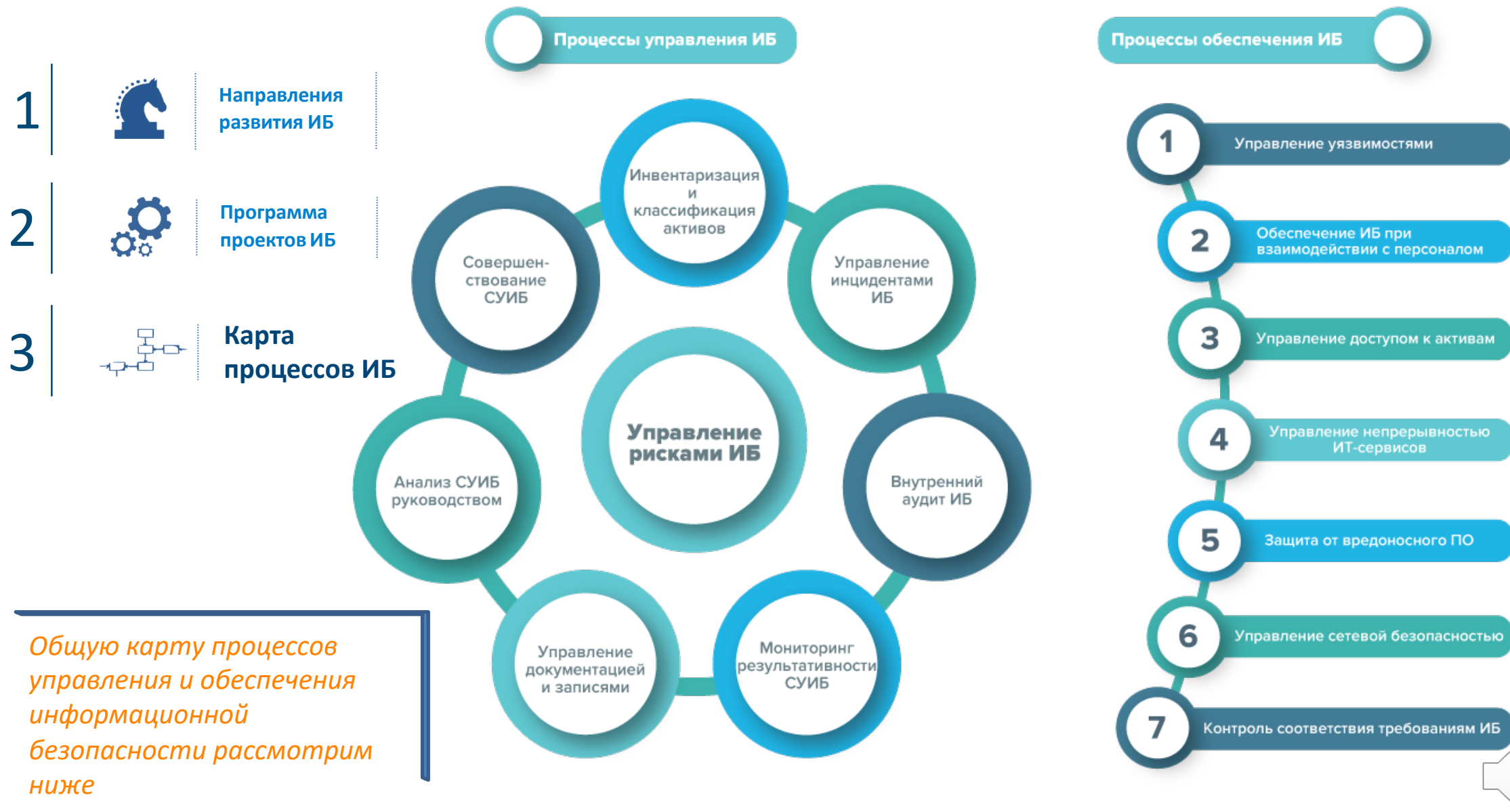


Основные постулаты Agile –методологии :

- Люди и взаимодействие важнее процессов и инструментов.
- Работающий продукт важнее исчерпывающей документации.
- Сотрудничество с Заказчиком важнее согласования условий контракта.
- Готовность к изменениям важнее следования первоначальному плану.



ДЕКОМПОЗИРУЕМ: ПРОЦЕССЫ (рассмотрим с позиции рисков)



ДЕКОМПОЗИРУЕМ: СТРУКТУРА

(BEST PRACTICE)



- 1 Направления развития ИБ
- 2 Программа проектов ИБ
- 3 Карта процессов ИБ
- 4 **Оргструктура комплексной системы ИБ**
(с позиции крупного предприятия)



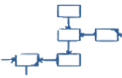
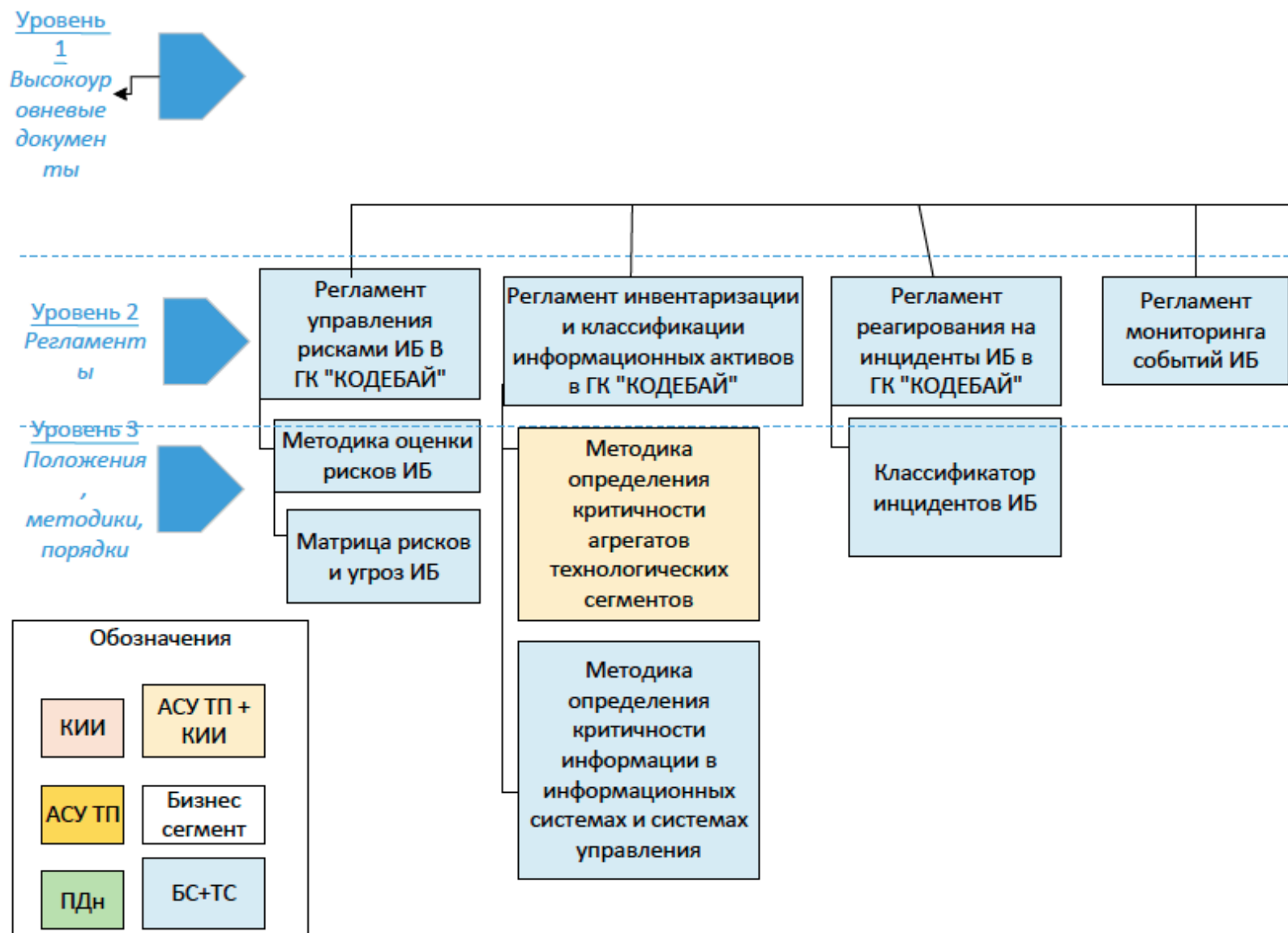
- 1  Направления развития ИБ
- 2  Программа проектов ИБ
- 3  Карта процессов ИБ
- 4  Оргструктура комплексной системы ИБ
- 5  Презентация Стратегии ИБ

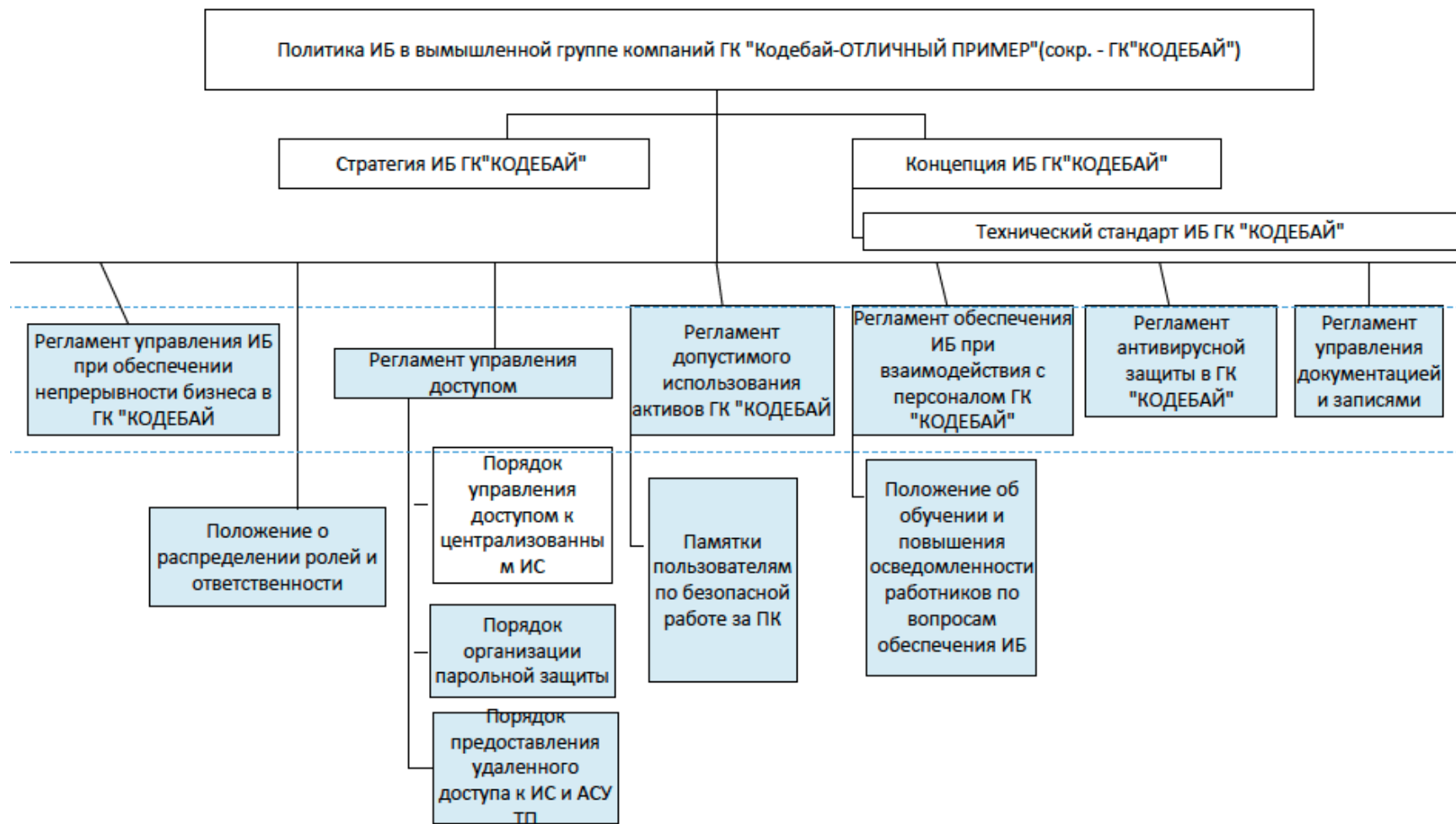


СХЕМА НПА В СОВРЕМЕННОЙ ОРГАНИЗАЦИИ. УРОВНИ НПА

(ДОКУМЕНТ В ПРИЛОЖЕНИИ)



СТРУКТУРА НПА ВЕРХНЕГО УРОВНЯ

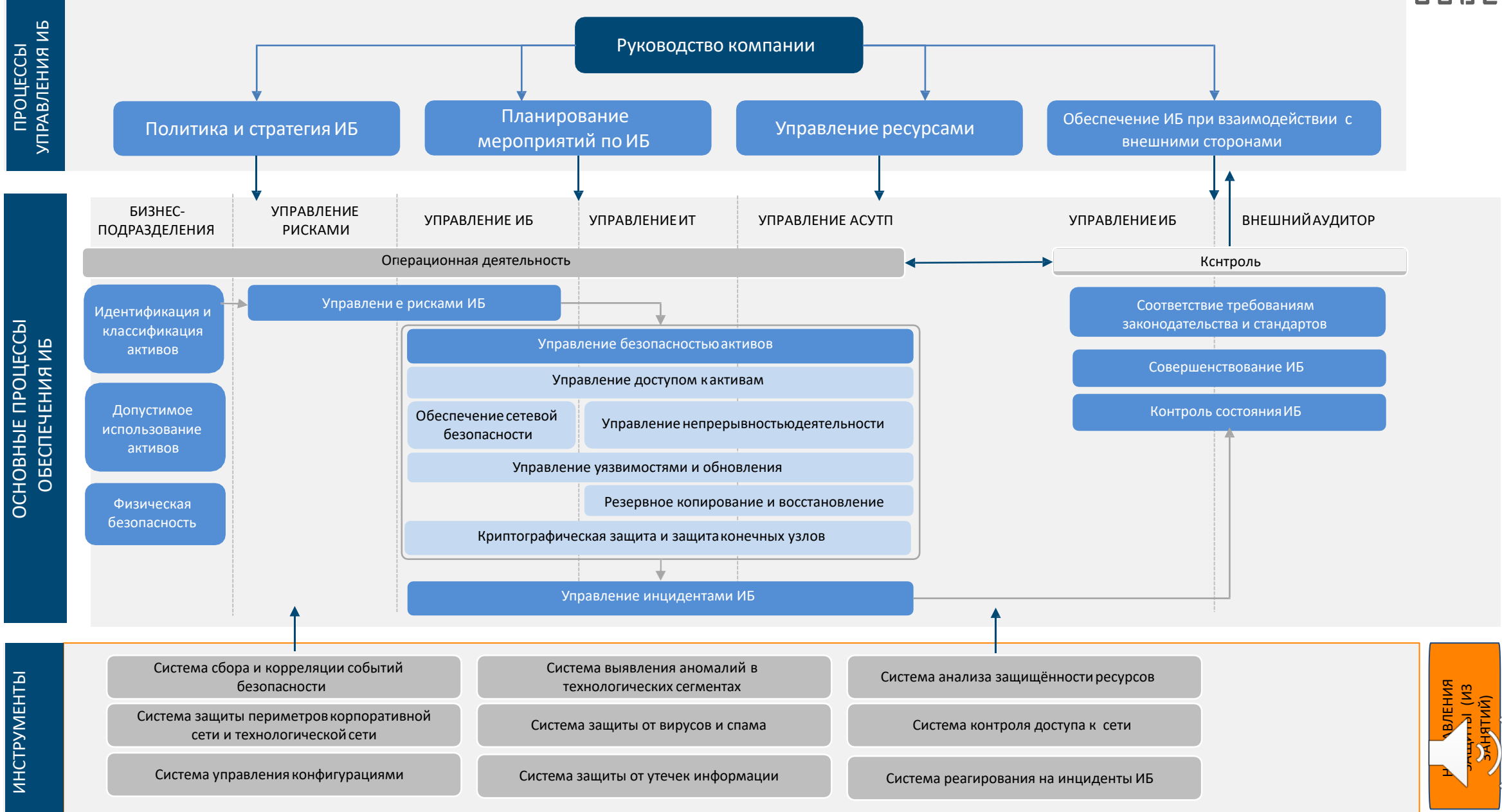


КАРТА ПРОЦЕССОВ УПРАВЛЕНИЯ И ОБЕСПЕЧЕНИЯ ИБ

(BEST PRACTICE)



КАРТА ПРОЦЕССОВ УПРАВЛЕНИЯ И ОБЕСПЕЧЕНИЯ ИБ



**Благодарю
за внимание!**

