



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

29 марта 2019 г.
г. Краснодар

#CODEIB

НОВОСТИ ЗАКОНОДАТЕЛЬСТВА И РЕГУЛИРОВАНИЯ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ



Сергей Борисов

Заместитель генерального директора по ИБ,
ООО “Информационные системы и аутсорсинг”

EMAIL: s.borisov@krasnodar.pro

БЛОГ: <https://sborisov.blogspot.ru/>

TWITTER: <https://twitter.com/sb0risov>



A wooden 3D puzzle spelling the word 'CODE' is the central focus, resting on a wooden desk. The puzzle is made of light-colored wood and is partially assembled. In the background, there are stacks of papers and a smartphone. In the foreground, several business cards are scattered on the desk. One card is clearly visible, featuring a QR code and the word 'УЧАСТНИК' (Participant) in Russian. The overall scene is dimly lit, with a warm, yellowish glow.

Персональные данные

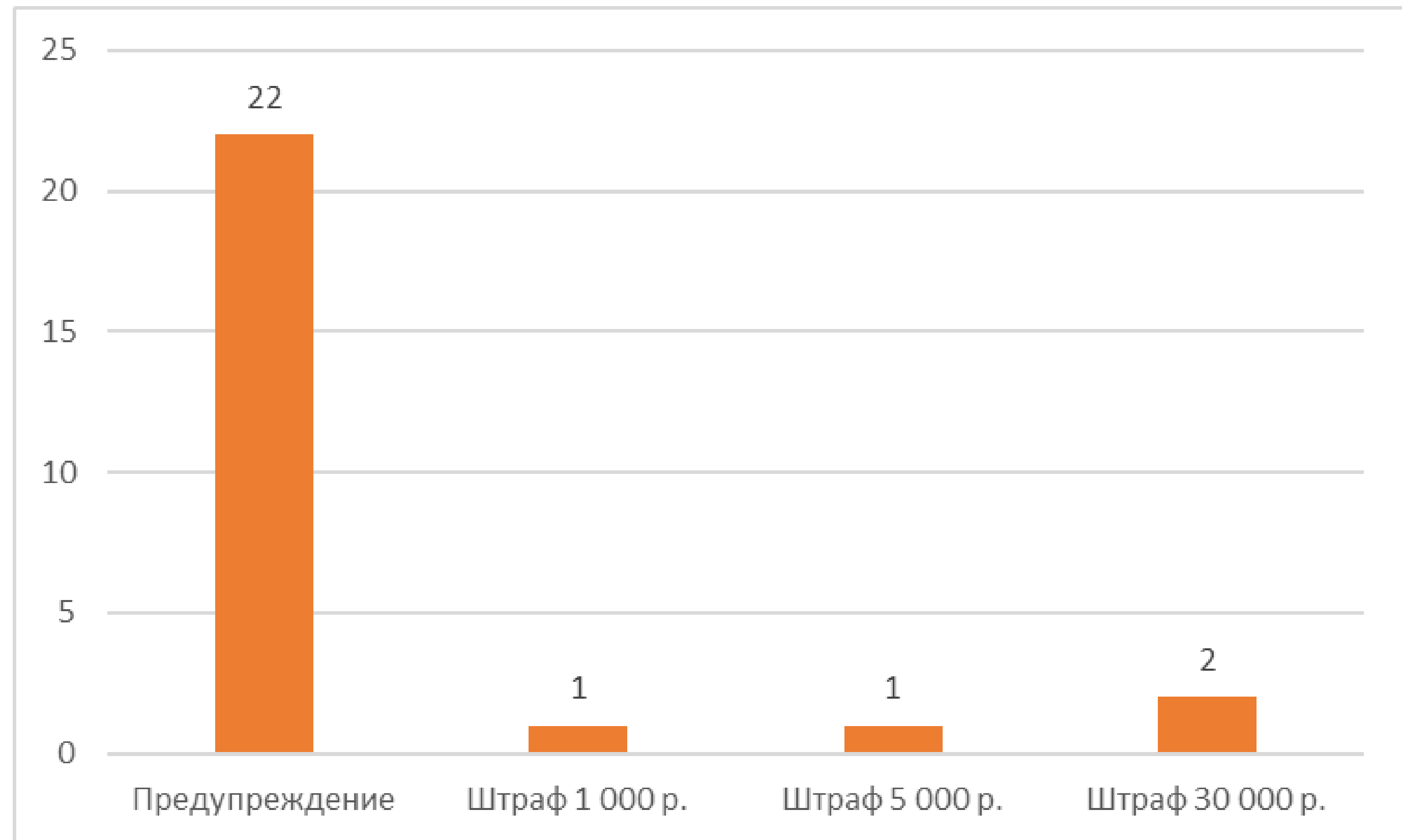
#CODEIB

Изменения в КОАП РФ

Пункт статьи 13.11 КоАП РФ	Штраф до		
	Гражданин	Должностное лицо	Юр. лицо
1. Обработка ПДн без оснований или несовместимая с целями сбора ПДн	3 тыс. руб.	10 тыс. руб.	50 тыс. руб.
2. Обработка ПДн без согласия (или неверное согласие) в письменной форме, когда оно необходимо	5 тыс. руб.	20 тыс. руб.	75 тыс. руб.
3. Не опубликование политики обработки и требований защиты	1 тыс. руб.	6 тыс. руб.	30 тыс. руб.
4. Не предоставление информации субъекту ПДн	2 тыс. руб.	6 тыс. руб.	40 тыс. руб.
5. Невыполнение законных требований субъекта ПДн по уточнению, блокированию или удалению	2 тыс. руб.	10 тыс. руб.	45 тыс. руб.
6. Невыполнение требований к безопасному хранению при неавтоматизированной обработке ПДн	2 тыс. руб.	10 тыс. руб.	50 тыс. руб.
7. Невыполнение обязанностей гос. и муниципальных органов по обезличиванию или нарушение правил обезличивания		6 тыс. руб.	
ИТОГО в случае множественных нарушений	15 тыс. руб.	68 тыс. руб.	290 тыс. руб.

Судебная практика по статье 13.11

СТАТИСТИКА ЗА
ПОСЛЕДНИЕ 4 МЕСЯЦА



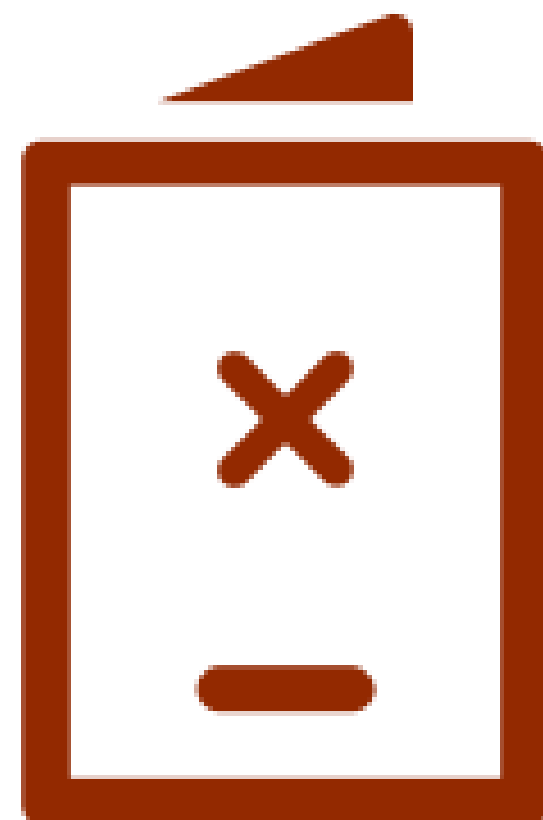
ОСВОБОЖДЕНИЕ ОТ ОТВЕТСТВЕННОСТИ - СТ. 2.9 КОАП РФ

[HTTPS://ROSPRAVOSUDIE.COM/DATE_FROM-2017-11-28/DATE_TO-2018-03-28/CATEGORY-13-11-S/VIDPR-ADMINISTRATIVNOE/SECTION-ACTS/](https://rospravosudie.com/date_from-2017-11-28/date_to-2018-03-28/category-13-11-s/vidpr-administrativnoe/section-acts/)

Изменения полномочий РКН

- + КОНТРОЛЬ ВЫПОЛНЕНИЯ НЕ ТОЛЬКО 152-ФЗ НО И ДРУГИХ НПА
- + НЕ ТОЛЬКО ОСУЩЕСТВЛЯЕТ КОНТРОЛЬ, НО ОРГАНИЗУЕТ И ОБЕСПЕЧИВАЕТ
- + НЕ СОГЛАСУЕТ С ПРОКУРОТУРОЙ ПРОВЕРКИ, НЕ ПУБЛИКУЕТ СВОДНЫЙ ПЛАН

Изменения полномочий РКН



ПРИКАЗ МИНКОМСВЯЗИ РОССИИ



ПРИКАЗ РОСКОНАДЗОРА

#CODEIB

Рекомендации РКН Политика обработки ПДн

+ ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ,
КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ **ДЛЯ КАЖДОЙ ЦЕЛИ**

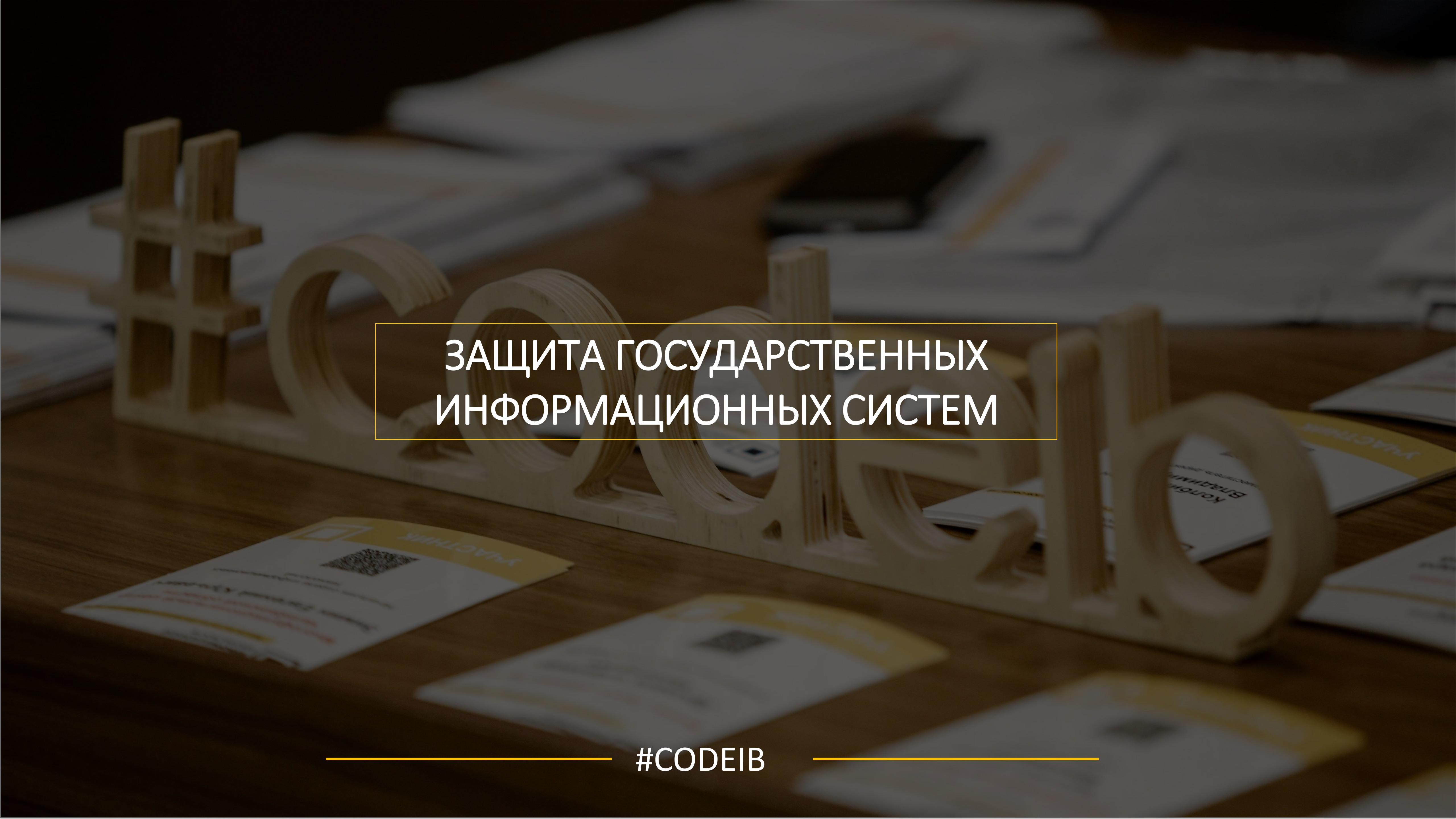


+ ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ
ДАННЫХ, В ТОМ ЧИСЛЕ: **ПЕРЕДАЧА ПДн ТРЕТЬИМ
ЛИЦАМ**, СРОКИ ХРАНЕНИЯ ПДн

+ ВЗАИМОДЕЙСТВИЕ С СУБЪЕКТАМИ ПДн

Изменения в 21 приказ ФСТЭК

Классы защиты сертифицированных СЗИ	УЗ 1	УЗ 2	УЗ 3	УЗ 4
1	+	+	+	+
2	+	+	+	+
3	+	+	+	+
4	+	+	+	+
5		+	+	+
6			+	+

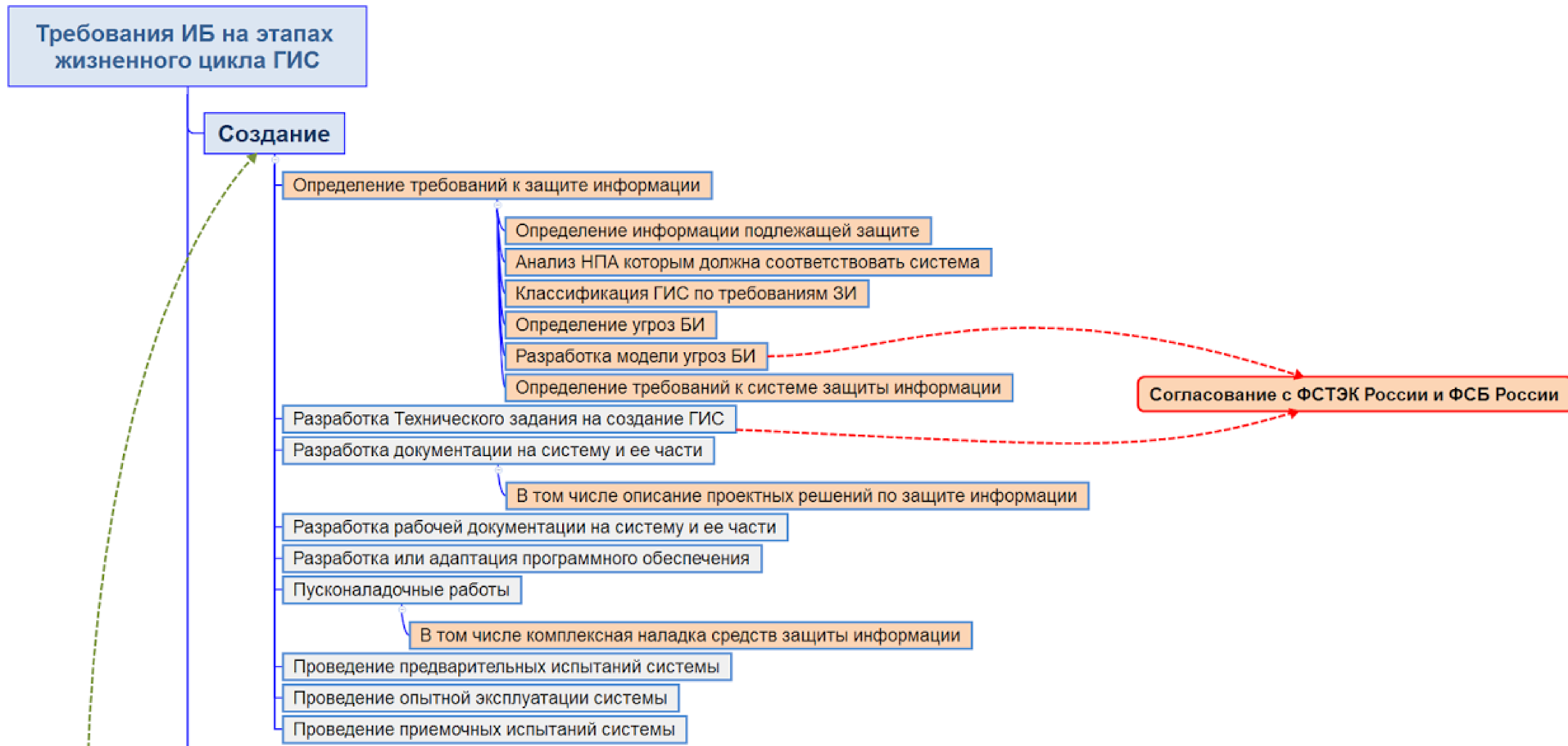


ЗАЩИТА ГОСУДАРСТВЕННЫХ
ИНФОРМАЦИОННЫХ СИСТЕМ

#CODEIB

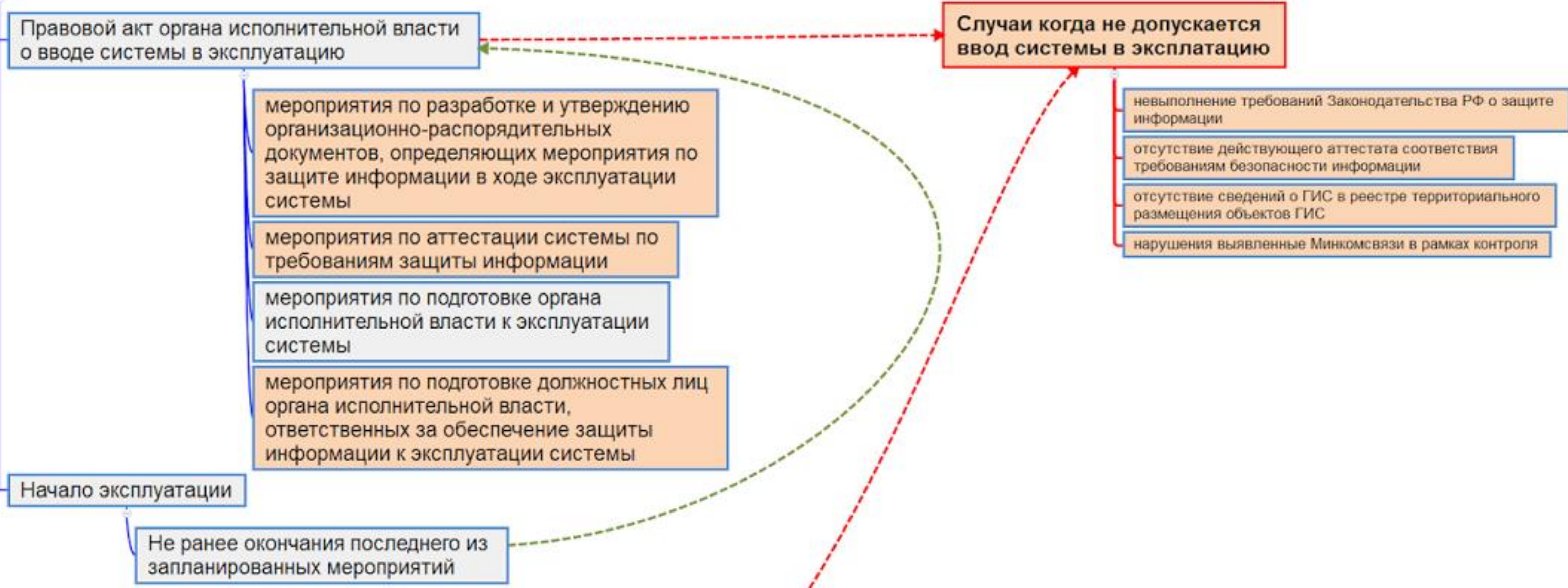
Изменение порядка создания и эксплуатации ГИС

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА №555



Изменение порядка создания и эксплуатации ГИС

Ввод в эксплуатацию



Изменение порядка создания и эксплуатации ГИС



Изменения в 17 приказ ФСТЭК

— УБРАЛИ ГИС КЛАССА К4.
ПОМЕНЯЛСЯ ПОРЯДОК КЛАССИФИКАЦИИ

+ АНАЛИЗ УЯЗВИМОСТЕЙ

+ ИСПОЛЬЗОВАТЬ БАНК ДАННЫХ УГРОЗ ФСТЭК
РОССИИ

+ НЕБОЛЬШИЕ ИЗМЕНЕНИЯ В БАЗОВЫХ НАБОРАХ
МЕР ЗАЩИТЫ


+ ОТДЕЛЬНАЯ АТТЕСТАЦИЯ ЦОД

+ ПОМЕНЯЛИСЬ ТРЕБОВАНИЯ К КЛАССАМ
ЗАЩИТЫ СЗИ

Изменения в 17 приказ ФСТЭК

Классы защиты сертифицированных СЗИ	К1	К2	К3
1	+	+	+
2	+	+	+
3	+	+	+
4	+	+	+
5		+	+
6			+

————— #CODEIB —————



БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ
ИНФОРМАЦИОННОЙ
ИНФРАСТРУКТУРЫ РФ

#CODEIB

ФЕДЕРАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО

- + **№187-ФЗ ОТ 26.07.2017 “О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ”**
- + **№193-ФЗ ВНОСЯТСЯ ИЗМЕНЕНИЯ В ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ «О ГОСУДАРСТВЕННОЙ ТАЙНЕ»**
- + **№194-ФЗ ДОПОЛНЯЕТ УГОЛОВНЫЙ КОДЕКС РФ СТАТЬЕЙ 274¹ «НЕПРАВОМЕРНОЕ ВОЗДЕЙСТВИЕ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

СФЕРА ДЕЙСТВИЯ ФЗ О БКИИ

ЗДРАВООХРАНЕНИЕ

НАУКА

ТРАНСПОРТ

СВЯЗЬ

ЭНЕРГЕТИКА

БАНКОВСКАЯ И ФИНАНСОВАЯ

ТЭК

АТОМНАЯ ЭНЕРГЕТИКА

ОБОРОННАЯ ПРОМЫШЛЕННОСТЬ

РАКЕТНО-КОСМИЧЕСКАЯ
ПРОМЫШЛЕННОСТЬ

ГОРНОДОБЫВАЮЩАЯ
ПРОМЫШЛЕННОСТЬ

МЕТАЛУРГИЧЕСКАЯ
ПРОМЫШЛЕННОСТЬ

ХИМИЧЕСКАЯ ПРОМЫШЛЕННОСТЬ

ЛИЦА КОТОРЫЕ ОБЕСПЕЧИВАЮТ
ВЗАИМОДЕЙСТВИЕ УКАЗАННЫХ
СИСТЕМ И СЕТЕЙ

ПОДЗАКОННЫЕ НПА

5 УКАЗОВ ПРЕЗИДЕНТА РФ

2 ПОСТАНОВЛЕНИЯ
ПРАВИТЕЛЬСТВА РФ

4 ПРИКАЗА ФСТЭК РОССИИ

6 ПРОЕКТА ПРИКАЗА ФСБ РОССИИ

2 ПРОЕКТА ПРИКАЗА ФСТЭК
РОССИИ

1 ПРОЕКТ ПРИКАЗА МИНКОМСВЯЗИ

КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ КИИ

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ №127 ОТ 08.02.2018



ТРЕБОВАНИЯ ФСТЭК РОССИИ

ПРИКАЗ ФСТЭК РОССИИ №235 ОТ 21.12.2017

ПРИКАЗ ФСТЭК РОССИИ №239 ОТ 25.12.2017

- + НЕДОПУСКАЕТСЯ ВОЗЛОЖЕНИЕ ОБЯЗАННОСТЕЙ НЕ СВЯЗАННЫХ С ИБ
- + ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ В ВОПРОСАХ ИБ НЕ РЕЖЕ 1 РАЗА В ГОД
- + СЗИ ДОЛЖНЫ БЫТЬ ОБЕСПЕЧЕНЫ ТЕХ. ПОДДЕРЖКОЙ
- + ОЦЕНКА СООТВЕТСТВИЯ: СЕРТИФИКАЦИЯ ИЛИ ИСПЫТАНИЯ (ПРИЕМКА)
- + ТРЕБОВАНИЯ К СОСТАВУ ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНОЙ ДОКУМЕНТАЦИИ
- + ЕЖЕГОДНОЕ ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ, КОНТРОЛЬ И ОТЧЕТНОСТЬ

ТРЕБОВАНИЯ ФСТЭК РОССИИ

ПРИКАЗ ФСТЭК РОССИИ №235 ОТ 21.12.2017

ПРИКАЗ ФСТЭК РОССИИ №239 ОТ 25.12.2017

+ ТРЕБОВАНИЯ К СОДЕРЖАНИЮ МОДЕЛЕЙ
УГРОЗ

+ ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ
В ВОПРОСАХ ИБ НЕ РЕЖЕ 1 РАЗА В ГОД

+ РАСШИРЕНЫ ТРЕБОВАНИЯ К АНАЛИЗУ УЯЗВИМОСТЕЙ
(ПЕНТЕСТЫ, АНАЛИЗ КОДА)

+ ЗАПРЕТ НЕКОНТРОЛИРУЕМОГО ДОСТУПА,
СБОРА ИНФОРМАЦИИ РАЗРАБОТЧИКОМ ПО / АС

+ СУЩЕСТВЕННОЕ ИЗМЕНЕНИЯ БАЗОВЫХ
НАБОРОВ МЕР ЗАЩИТЫ:
166 → 152
ДЛЯ 3 КАТЕГОРИИ: 94 → 86

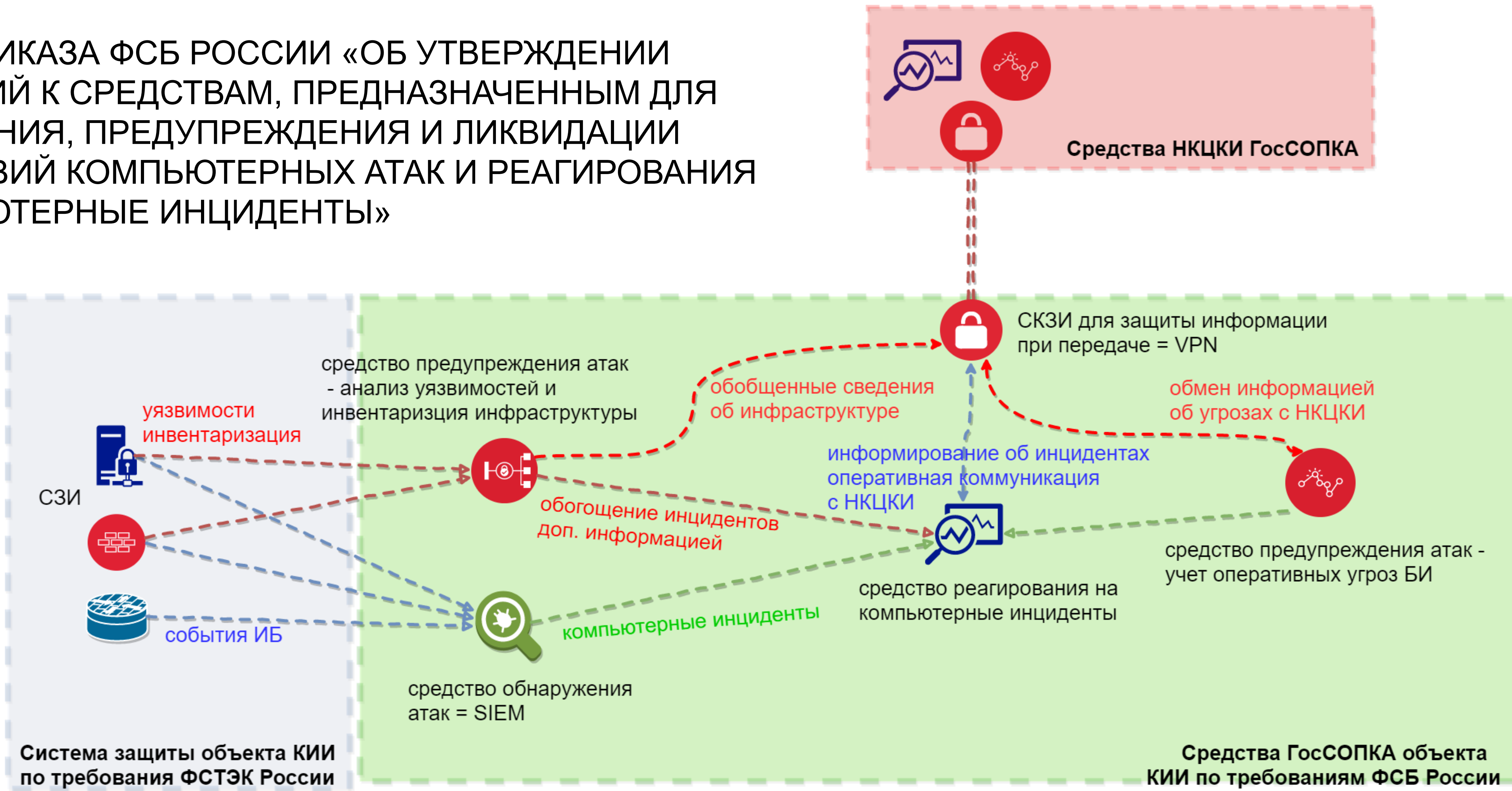
+ НОВЫЕ МЕРЫ: ИНВЕНТАРИЗАЦИЯ РЕСУРСОВ, АНАЛИЗ СЕТЕВОГО ТРАФИКА, АУДИТЫ ИБ,
ЭШЕЛОНИРОВАННАЯ ЗАЩИТА, ДМЗ, ПЕСОЧНИЦЫ

ТРЕБОВАНИЯ ФСТЭК РОССИИ

Приказ ФСТЭК №31					Сравнение	Новый приказ ФСТЭК №239					Анализ нового
Условное обозначение и номер меры	Меры защиты информации в автоматизированных системах управления	Классы защищенности				Условное обозначение и номер меры	Меры обеспечения безопасности	Категория значимости			
		3	2	1	3			2	1		
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)						I. Идентификация и аутентификация (ИАФ)					
ИАФ.0	Разработка правил и процедур (политик) идентификации и аутентификации субъектов доступа и объектов доступа	+	+	+		ИАФ.0	Разработка политики идентификации и аутентификации	+	+	+	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+		ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+	
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных		+	+		ИАФ.2	Идентификация и аутентификация устройств	+	+	+	
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, изменение, уничтожение идентификаторов	+	+	+		ИАФ.3	Управление идентификаторами	+	+	+	
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+		ИАФ.4	Управление аутентификаторами	+	+	+	
ИАФ.5	Исключение отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых символов (защита обратной связи при вводе аутентификационной информации)	+	+	+	Удалено	ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+	Из ИАФ.6
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	В ИАФ.5	ИАФ.6	Двусторонняя аутентификация				Новое
ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа				Удалено	ИАФ.7	Защита аутентификационной информации при передаче	+	+	+	Новое

ТРЕБОВАНИЯ ФСБ РОССИИ

ПРОЕКТ ПРИКАЗА ФСБ РОССИИ «ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К СРЕДСТВАМ, ПРЕДНАЗНАЧЕННЫМ ДЛЯ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК И РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ»





КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

29 марта 2019 г.
г. Краснодар

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ!!



Сергей Борисов

Заместитель генерального директора по ИБ,
ООО "Информационные системы и аутсорсинг"

EMAIL: s.borisov@krasnodar.pro

БЛОГ: <https://sborisov.blogspot.ru/>

TWITTER: <https://twitter.com/sb0risov>

